SUNCORPORATION

通信モジュール一体型ルータ

取扱説明書

http://www.sun-denshi.co.jp/sc/

はじめに

表記について

本取扱説明書では、安全にお使いいただくために、守っていただきたい事項に次のマークを表示しております。

人体に危険を及ぼしたり、装置に大きなダメージを与えたりする可能性があることを示しています。必ずお守りください。

機能停止を招いたり、各種データを消してしまったりする可能性があることを示しています。十分に注意してください。

関連する情報を記載しています。参考にお読みください。

製品名について

本取扱説明書では、「Rooster RX110」「Rooster RX130」「Rooster RX160」「Rooster RX180」を「Rooster RX」と省略して記載しております。各機種の対応機能については、対応機能一覧をご覧ください。

商標について

「Rooster」は、サン電子株式会社の登録商標および商標登録出願中です。
「FOMA」「moperaU」「エリアメール」は、NTT ドコモの商標または登録商標です。
「SOFTBANK」および「ソフトバンク」の名称、ロゴは日本国およびその他の国におけるソフトバンク株式会社の登録商標または商標です。
「au」は、KDDI 株式会社の商標または登録商標です。
「4G LTE」は、国際電気通信連合(ITU)が LTE を「4G」と呼称することを認めた声明に準じております。
Windows は米国 Microsoft Corporation の米国およびその他の国における登録商標です。
その他、本取扱説明書に記載されている会社名、製品名は、各社の商標または登録商標です。
本文中の各社の商標または登録商標には、TM、®マークは表示しておりません。

GPL／LGPLライセンスについて

本製品は、GPL version2.0／LGPL version2.0 の適用ソフトウェアを使用しております。オープンソースとしての性格上著作権による保証はなされておりませんが、本製品につきましては保証書、および取扱説明書記載の条件により当社による保証がなされています。GPL／LGPL のライセンスにつきましては、以下の URL をご覧ください。

- http://www.gnu.org/licenses/gpl-2.0.html
- http://www.gnu.org/licenses/lgpl-2.0.html

変更済み GPL 対象モジュール、その配布方法につきましては、サン電子（株）サポートセンターにご連絡ください。なお、配布時発生する費用はお客様のご負担となります。

本取扱説明書の画面イメージは開発中のものです。
実際の画面とは多少異なる場合があります。

安全上のご注意（必ずお守りください）

ここに記載している注意事項は、安全に関わる重要な内容ですので、必ず守ってください。本取扱説明書では、安全上の注意事項を「警告」と「注意」に区分しています。

警告	この表示を無視して、間違った取り扱いをした場合、人が死亡または重傷を負う可能性が想定される内容を示しています。
注意	この表示を無視して、間違った取り扱いをした場合、人が損害を負う可能性が想定される内容、および物的損害のみの発生が想定される内容を示しています。物的損害とは、家屋、家財および家畜、ペットに関する拡大損害を示しています。
	禁止行為（してはいけないこと）を示しています。
	強制行為（必ずしなければいけないこと）を示しています。

なお、注意、禁止に記載した事項でも、状況によっては重大な結果に結びつく場合があります。いずれも重要な内容を記載していますので、必ず守ってください。

警 告

分解禁止

本製品を分解したり、改造したりしないでください。

➔ 感電、火災、故障の原因になります。

禁止

近くに雷が発生したときには AC アダプタを本体から抜いてご使用をお控えください。

➔ 落雷が火災、感電、故障の原因となるときがあります。

禁止

本製品に水などの液体をかけたり、異物を入れたりしないでください。

➔ 感電や火災、故障の原因になります。万一、本製品に液体がかかったり、異物が入ったりした場合は、AC アダプタをコンセントから抜いて、点検修理を依頼してください。

強制

製品から煙、異臭、異常音が発生した場合は、AC アダプタをコンセントから抜き、本製品を接続している機器からケーブルを取り外してください。また、点検修理を依頼してください。

➔ 火災の原因になります。

禁止

電源ケーブルを傷つけないでください。

➔ 感電、火災の原因になります。

強制

AC アダプタは、AC100V コンセントに接続してください。また、本製品を設置、移動する時は、電源プラグを抜いてください。

➔ 故障、火災の原因になります。

禁止

梱包のポリ袋などは、小さいお子様の手の届く所に置かないでください。

➔ 小さいお子様がかぶったり、飲みこんだりすると、呼吸を妨げる危険があります。

強制

電源プラグは確実に根元まで差し込んでください。また、電源プラグとコンセントの間のほこりは、定期的（半年に一回程度）に取り除いてください。

➔ 電源プラグの間にほこりが付着し、電源が短絡して発煙、発火、火災の恐れがあります。

禁止

強い衝撃を与えたり、落下させたり、投げ付けたりしないでください。

➔ 機器の故障、火災の原因となります。

禁止

ガソリンスタンドなど、引火、爆発の恐れがある場所では、使用しないでください。

➔ プロパンガス、ガソリンなど引火性ガスや粉塵が発生する場所で使用すると、爆発や火災の原因となります。

禁止

電子レンジなどの加熱調理機や高圧容器に、本装置を入れないでください。

➔ 機器の発熱、発煙、発火や回路部品を破損させる原因となります。

強制

指定アンテナ以外の外部アンテナを接続しないでください。

➔ 指定以外の外部アンテナを接続した場合、電波法の規定に抵触する可能性があります。

⚠注 意

禁止

この取扱説明書に記載されている周囲環境条件以外では、使用、保管しないでください。

➔ 本製品の故障や破損などによって、発煙、発火、感電の原因になります。下記の環境には、特にご注意ください。

- 室内または製品周囲の温度や湿度が極端に高い、または低い場所
- 結露がある場所
- 急激な温度変化が起きる場所
- ほこりが多い場所
- 静電気が発生しやすい場所
- 腐食性のガスが発生する場所
- 水などがかかりやすい場所
- 振動や衝撃が加わるような不安定な場所
- 油煙が当たる場所
- 直射日光が当たる場所
- 製品周囲に発熱する器具や燃えやすい物がある場所
- 周囲に置いてある物との間に適切な空間がない場所

禁止

専用の AC アダプタまたは規格に合った電源以外を使用しないでください。

➔ 他の電源を使用すると、故障、火災の原因になります。

強制

30cm 以上の高さから落とした場合は、使用を中止し、点検、修理を依頼してください。

➔ そのまま使用すると、重大な事故になる可能性があります。

禁止

本製品は日本国内向けに設計されています。

➔ 海外ではご使用にならないでください。

医用電気機器近くでの取り扱いについて

本記載の内容は「医用電気機器への電波の影響を防止するための携帯電話端末等の使用に関する指針」（電波環境協議会）に準拠したものです。

⚠ 警 告

強制

医療機関の屋内では次のことを守って使用してください。

- 手術室、集中治療室（ICU）、冠状動脈疾患監視病室（CCU）には本装置を持ち込まないでください。
- 病棟内では、本装置を使用しないでください。
- ロビーなどであっても付近に医用電気機器がある場合は、本装置を使用しないでください。
- 医療機関が個々に使用禁止、持ち込み禁止などの場所を定めている場合は、その医療機関の指示に従ってください。

強制

満員電車の中など混雑した場所では、付近に植込み型心臓ペースメーカおよび植込み型除細動器を装着している方がいる可能性がありますので、本装置の電源を切ってください。

➔ 電波により植込み型心臓ペースメーカおよび植込み型除細動器の作動に悪影響を及ぼす原因となります。

強制

植込み型心臓ペースメーカおよび植込み型除細動器を装着されている場合は、装着部から本装置の外部アンテナを 22cm 以上離して携行および使用してください。

➔ 電波により植込み型心臓ペースメーカおよび植込み型除細動器の作動に悪影響を及ぼす原因となります。

強制

自宅療養など医療機関の外で、植込み型心臓ペースメーカおよび植込み型除細動器以外の医用電気機器を使用される場合には、電波による影響について個別に医用電気機器メーカなどにご確認ください。

➔ 電波により医用電気機器の作動に悪影響を及ぼす原因となります。

ご使用時の取り扱いについて

ご使用にあたってのお願い

- 本製品周辺で静電気的障害を発生させないでください。
  ➔ 本製品は、静電気に敏感な部品を使用しています。特に、コネクタの接点、ポート、その他の部品に、素手で触れないでください。部品が静電破壊するおそれがあります。
- 本製品はていねいに取り扱ってください。
  ➔ 本製品に強いショックを与えると破損の原因になります。
- 本製品のお手入れは、電源を切った状態で行ってください。
  ➔ 誤動作や故障の原因になります。
- 本製品のお手入れには、揮発性の有機溶剤、薬品、化学ぞうきんなどを使用せず、乾いた柔らかい布で拭いてください。汚れがひどい場合は、柔らかい布に台所中性洗剤をしみこませて固く絞ってから拭き、最後に乾いた柔らかい布で仕上げてください。
  ➔ 揮発性の有機溶剤、薬品、化学ぞうきんなどを使用すると、変質、変色、場合によっては破損の原因になります。
- 極端な高温、低温は避けてください。
  ➔ 温度は-20～60℃、湿度は 25～85%の範囲でご使用ください。
- 使用中、本装置が温かくなることがありますが、異常ではありませんのでそのままご使用ください。
- 長い時間連続して通信をした場合など、本装置が熱くなることがありますので取り扱いにご注意ください。
- 一般の電話機やテレビ・ラジオなどをお使いになっている近くで使用すると、影響を与える場合がありますので、なるべく離れた場所でご使用ください。
- お使いになる環境や接続する外部装置によっては、本装置がノイズによる影響を受け、無線特性が劣化する場合があります。
- 本装置に貼付してある銘版シール（製造番号等印字シール）を剥がさないでください。
  ➔ 本シールは、技術基準適合証明、技術基準適合認証を取得していることを示すものであり、剥がした状態での使用は法律で禁止されています。
- 本装置に貼付してある水濡れシールを剥がさないでください。
  ➔ 本シールは、水濡れを確認するものであり、剥がした状態では保証対象外ですので有償修理となります。

お客様が本装置を利用して公衆に著しく迷惑をかける不良行為を行った場合、法律、条例（迷惑防止条例等）に従い処罰されることがあります。

地球環境保全のため、次のことにご協力ください。
- 本製品および付属品は、不燃物として処分してください。
- 廃棄方法は、地方自治体などで決められた分別収集方法に従ってください。
- 一般ごみとして、家庭で焼却処分しないでください。
- ダイオキシンや塩化水素ガスなどが発生し、環境や人体に影響を与えます。

ご注意

- 本製品の仕様は国内向けになっておりますので、海外ではご利用になれません。
  These products are designed for use in Japan only and cannot be used in any other countries.
- 本製品を医用電気機器や幹線通信機器、電算機システムなどの、きわめて高い安全性や信頼性が要求される用途には使用しないでください。
- 取扱説明書について、次の点にご注意ください。
  1. 本製品は無線によるデータ通信を行う事が出来る装置です。本製品の不具合、誤動作又は停電、回線障害、その他の外部要因によって通信障害が発生したために生じた損害等については、当社としては責任を負いかねますので、あらかじめご了承ください。
  2. 本取扱説明書の内容の一部または全部を、無断で転載することを禁止します。
  3. 本取扱説明書の内容に関しては、将来予告なしに変更される場合があります。
  4. 本取扱説明書の内容につきましては、万全を期して作成致しましたが、万一ご不審な点や、ご不明な点、誤り、記載漏れ、乱丁、落丁、その他お気づきの点等ございましたら、当社までご連絡ください。
  5. 適用した結果の影響につきましては、4 項にかかわらず責任を負いかねますので、ご了承ください。
  6. 本取扱説明書で指示されている内容につきましては、必ず従ってください。本取扱説明書に記載されている内容を無視した行為や誤った操作によって生じた障害や損害につきましては、保証期間内であっても責任を負いかねますので、ご了承ください。

本装置使用時に注意すべきことについて

本製品に電源を供給して使用した場合、下記の事項を注意することを推奨いたします。

- 高精度な制御や微弱な信号を取り扱う電子機器の近くでは、本装置の電源を切れる構造とすることをお奨めします。
  ➔ 電子機器が誤作動するなど影響を与える可能性があります。

  【ご注意いただきたい電子機器の例】
  補聴器、植込み型心臓ペースメーカおよび植込み型除細動器、その他医用電気機器、火災報知機、自動ドア、その他の自動制御機器など

  ➔ 参考：「医用電気機器への電波の影響を防止するための携帯電話端末等の使用に関する指針」（電波環境協議会［平成 9 年 4 月］）
- 本装置は、自動車内、航空機内、医療機関内のご使用を想定した設計はしていません。
  ➔ 本装置を自動車内、航空機内、医療機関内に持ち込まれる場合は、高精度な制御や微弱な信号を取り扱う電子機器に影響を与える可能性があります。
  本装置の電源を切れる構造として、他の機器に影響のないようにしてください。
- 本装置は日本国内での使用を想定して設計しています。
  ➔ 海外でのご使用をお考えの場合は、弊社までご相談ください。

ご使用機種の対応機能について

機種毎の対応機能一覧

本マニュアルは、RX シリーズ全製品に共通するマニュアルです。
お使いの RX がどの機能に対応しているかは、下記の対応表でご確認ください。また、各機能の中で機種により差分がある箇所には、下記の機種マークで場合分けして記載しております。

RX110 RX130 RX160 RX180

機能 / 機種	RX110	RX130	RX160	RX180
時刻設定	○	○	○	○
おやすみモード	○	○	○	○
電源制御	○	○	○	○
WAN	○	○	○	○
ダイヤルアップ	○	○	○	○
RAS 着信	○	○	○	○※1
WakeOn 着信	○	○	○	○
アドレス解決	○	○	○	○
DNS	○	○	○	○
DHCP	○	○	○	○
TELNET	○	○	○	○
WEB	○	○	○	○
SNMP	○	○	○	○
WAN ハートビート	○	○	○	○
ログ管理	○	○	○	○
PPTP パススルー	○	○	○	○
IPsec パススルー	○	○	○	○
スタティックルーティング	○	○	○	○
フィルタリング	○	○	○	○
バーチャルサーバ	○	○	○	○
DMZ	○	○	○	○
IPsec	○	○	○	○
PPTP	○	○	○	○
L2TP/IPsec	○※3	○※3	○※3	○※3
緊急速報受信	—	○※2	—	—
OTA	—	—	○	—
位置測位	—	—	○※3	—

※1.　FW バージョン v1.2.0 より対応。
※2.　FW バージョン v1.2.0 より対応。NTT ドコモの呼称は「エリアメール」です。
※3.　FW バージョン v1.4.0 より対応。

無線LAN対応について

無線 LAN 対応機種における無線 LAN 機能については、「RoosterRX 取扱説明書（無線 LAN 版）」をご覧ください。

目次

1章　Rooster RXの概要

この章では、Rooster RX の概要や特長、外観などについて説明します。

1-1 概要

RX110

本製品は 3G 通信モジュールを内蔵したルータです。
株式会社 NTT ドコモ社 FOMA パケット通信サービスを利用しパケット通信を行うことができます。
本製品では、通信モジュール「LISA-U200」をモバイル通信端末と記載しています。
本製品を FOMA ネットワークへ接続するためには、「FOMA サービス」のご契約と、FOMA SIM カードを内部 SIM カードソケットに装着する必要があります。

本製品には、電気通信事業法第 56 条第 1 項の規定に基づく端末機器の設計について認証を受けた以下の設備が組み込まれております。
- 機器名称：LISA-U200、認定番号：AD120274003

本製品には、特定無線設備の技術基準適合証明等に関する規制第 2 条第 1 項第 11 号の 3 に規定される以下の設備が組み込まれております。
- 機器名称：LISA-U200、工事設計認証番号：003-120375

本製品には、特定無線設備の技術基準適合証明等に関する規制第 2 条第 1 項第 11 号の 7 に規定される以下の設備が組み込まれております。
- 機器名称：LISA-U200、工事設計認証番号：003-120375

RX130

本製品は 3G 通信モジュールを内蔵したルータです。
株式会社 NTT ドコモ社 FOMA パケット通信サービスを利用しパケット通信を行うことができます。
本製品では、通信モジュール「FOMA UM03-KO」をモバイル通信端末と記載しています。
本製品を FOMA ネットワークへ接続するためには、「FOMA サービス」のご契約と、FOMA SIM カードを内部 SIM カードソケットに装着する必要があります。

本製品には、電気通信事業法第 56 条第 2 項の規定に基づく端末機器の設計について認証を受けた以下の設備が組み込まれております。
- 機器名称：FOMA UM03-KO、認定番号：AD12-0227001

本製品には、特定無線設備の技術基準適合証明等に関する規制第 2 条第 1 項第 11 号の 3 および 7 に規定される以下の設備が組み込まれております。
- 機器名称：FOMA UM03-KO、工事設計認証番号：001-A00248

RX160

本製品は 4G LTE 通信モジュールを内蔵したルータです。
au 4G LTE 通信サービスを利用しパケット通信を行うことができます。
本製品では、通信モジュール「KYM11」をモバイル通信端末と記載しています。
本製品を au 4G LTE ネットワークへ接続するためには、KDDI 社のご契約が必要になります。(契約によっては、SIM カードを内部 SIM カードソケットに装着する必要があります)

本製品には、電気通信事業法第 56 条第 1 項の規定に基づく端末機器の設計について認証を受けた以下の設備が組み込まれております。

- 機器名称：KYM11、認定番号：D13-0207005

本製品には、特定無線設備の技術基準適合証明等に関する規制第 2 条第 1 項第 11 号の 3 に規定される以下の設備が組み込まれております。

- 機器名称：KYM11、工事設計認証番号：005-100609

本製品には、特定無線設備の技術基準適合証明等に関する規制第 2 条第 1 項第 11 号の 7 に規定される以下の設備が組み込まれております。

- 機器名称：KYM11、工事設計認証番号：005-100609

RX180

本製品は 3G 通信モジュールを内蔵したルータです。
株式会社ソフトバンクモバイル社ソフトバンクモバイル3G通信サービスを利用しパケット通信を行うことができます。
本製品では、通信モジュール「LISA-U270」をモバイル通信端末と記載しています。
本製品をソフトバンクモバイル 3G ネットワークへ接続するためには、ソフトバンク社のご契約と、SIM カードを内部 SIM カードソケットに装着する必要があります。

本製品には、電気通信事業法第 56 条第 1 項の規定に基づく端末機器の設計について認証を受けた以下の設備が組み込まれております。

- 機器名称：LISA-U270、認定番号：AD120274003

本製品には、特定無線設備の技術基準適合証明等に関する規制第 2 条第 1 項第 11 号の 3 に規定される以下の設備が組み込まれております。

- 機器名称：LISA-U270、工事設計認証番号：003-120377

本製品には、特定無線設備の技術基準適合証明等に関する規制第 2 条第 1 項第 11 号の 7 に規定される以下の設備が組み込まれております。

- 機器名称：LISA-U270、工事設計認証番号：003-120377

1-2 主な特長

高速パケット通信に対応

RX110

上り 5.7Mbps／下り 7.2Mbps の高速パケット通信に対応した u-blox 社製通信モジュール「LISA-U200」を内蔵し、NTT ドコモの FOMA 網で利用可能です。

RX130

上り 5.7Mbps／下り 7.2Mbps の高速パケット通信に対応した日立国際電気社製通信モジュール「FOMA UM03-KO」を内蔵し、NTT ドコモの FOMA 網で利用可能です。

RX160

上り 25Mbps／下り 75Mbps の高速パケット通信に対応した京セラ社製通信モジュール「KYM11」を内蔵し、KDDI の通信網で利用可能です。

RX180

上り 5.7Mbps／下り 7.2Mbps の高速パケット通信に対応した u-blox 社製通信モジュール「LISA-U270」を内蔵し、ソフトバンクモバイルの通信網で利用可能です。

有線接続に対応

モバイル通信だけでなく、ブロードバンドなどの有線接続に対応しました。

PPTP接続によるリモートメンテナンスが可能

PC から手軽に RX のリモートメンテナンスを可能とする PPTP サーバを搭載しました。

L2TP/IPsec接続によるリモートメンテナンスが可能

PC から手軽に RX のリモートメンテナンスを可能とする L2TP/IPsec サーバを搭載しました。

低消費電力を実現

従来機（H100）と比べ消費電力を 70%ダウンしました。
また、待機時更に低消費電力状態（0.3W）となる「おやすみモード」を搭載しました。

広い温度範囲、各種電源電圧に対応可能

動作温度範囲を-20～60℃とし、電源電圧も 5～24Ｖを実現し、幅広い利用環境に対応しました。

外付けアンテナに対応

SMA タイプのアンテナコネクタを搭載し、ルーフトップアンテナや小型アンテナ、防滴アンテナなど利用する環境に合わせ、各種外付けアンテナを選択することができます。

▶ 弊社よりオプションとしてご用意しております。

コンパクトな筐体サイズを実現

筐体は 127（W）×81（D）×22（H）mm のコンパクトなサイズを実現、更に設置環境の幅を広げました。

IPsec機能を標準搭載

Rooster RX ではメインモード／アグレッシブモードの各モードに対応した IPsec（暗号化アルゴリズム：AES256bit、3DES）機能を搭載し、モバイル通信網を利用した高セキュリティな多拠点ネットワークを構築することが可能です。

長期間の安定運用

過去の Rooster で実現した、無人環境においても長期間での安定した運用が可能となる機能を継承しています。RX 自身のヘルスチェックとして筐体内部の温度・供給電源電圧の監視が可能です。

緊急速報受信に対応 RX130

気象庁が配信する「緊急速報」や「津波警報」、国・地方公共団体が配信する「災害・避難情報」の注意喚起メッセージを受信することが可能です。

位置測位に対応 RX160

位置測位機能に対応しました。これにより、おおまかな＜緯度＞,＜経度＞,＜標高＞を取得することが可能です。

1-3 設定フロー

Rooster RX を使用してダイヤルアップ接続を行う場合、最低限 2 までの設定を行ってください。3 の設定は、必要に応じて行ってください。

1. Rooster RX の設置
   - 同梱品の確認

     ➲『1-4　同梱品の確認』
   - 機器の接続

     ➲『2-3　Rooster RX の接続方法』
   - クライアント PC の設定

     ➲『2-6　パソコンの設定』

2. Rooster RX の基本設定
   - LAN、ログインパスワード、時刻、メールアカウントの設定

     ➲『3-2　LAN の設定』

     ➲『3-3　ログインパスワードの設定』

     ➲『3-4　時刻の設定』

     ➲『3-5　メールアカウントの設定』
   - ダイヤルアップ接続設定

     ➲『4 章　ダイヤルアップ設定』

3. Rooster RX の詳細設定（必要な場合のみ）
   - 着信設定

     ➲『5 章　着信設定』
   - 各種サービス設定

     ➲『7 章　各種サービス設定』
   - ネットワーク設定

     ➲『8 章　ネットワーク設定』
   - VPN 設定

     ➲『8-6　IPsec』

1-4 同梱品の確認

パッケージには、次のものが同梱されています。

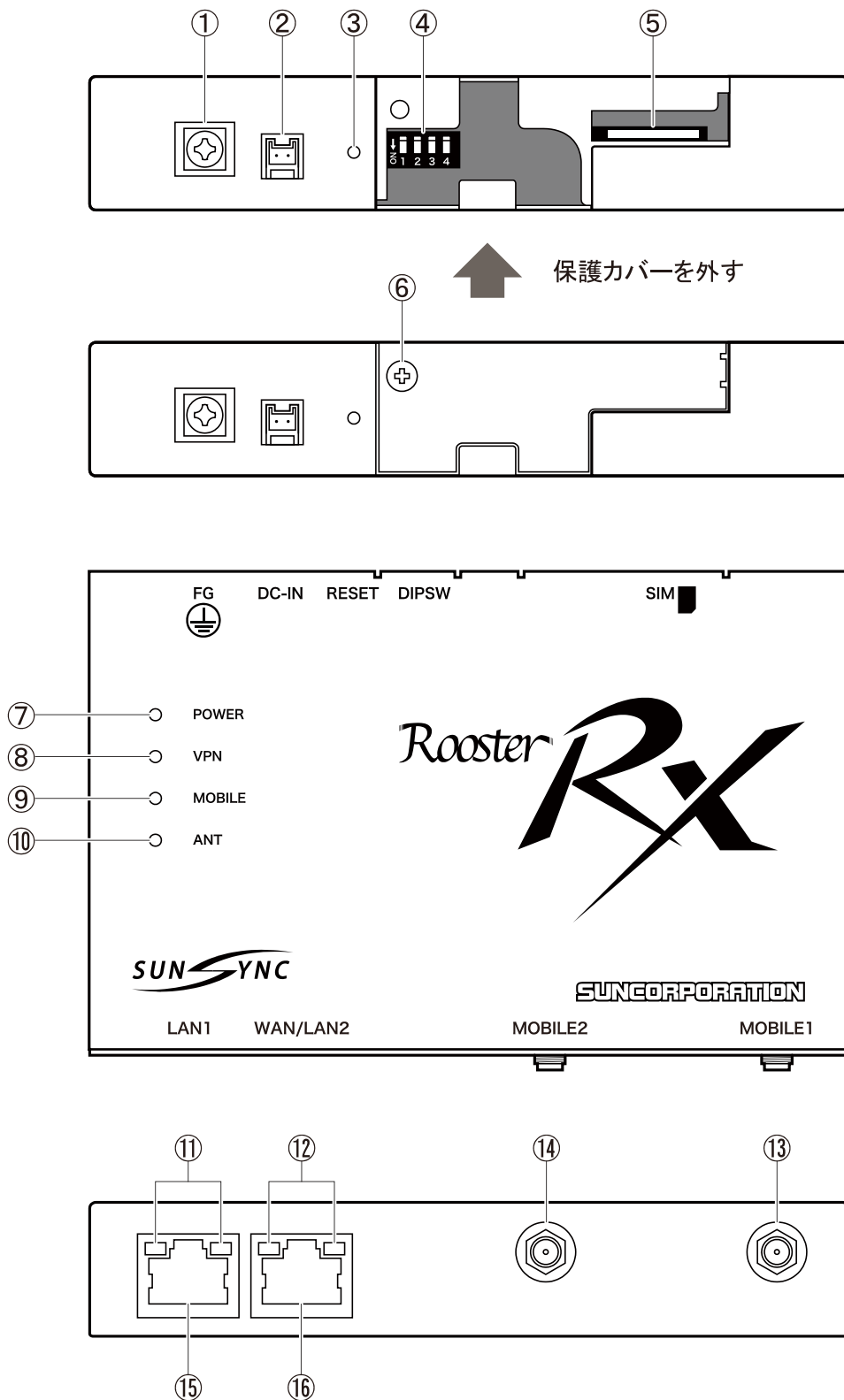
万一不足しているものがありましたら、お買い求めの販売店、もしくはサポートセンターにご連絡ください。

Rooster RX

- Rooster RX 本体　1 台
- スタートアップマニュアル（保証書付）　1 部

付属品に LAN ケーブル、アンテナおよび AC アダプタは含まれません。設定で使用する LAN ケーブルにつきましてはご利用の接続機器の速度に合わせてご用意ください。

- LAN ケーブル：
  100BASE-TX→カテゴリ 5
- アンテナ、AC アダプタ：
  オプション品として取り扱っております。弊社サポートまでお問い合わせください。

1-5 各部の名称と機能

[RX160 の場合]

No.	名称	機能
①	FG 端子	アース線を接続します。
②	DC IN コネクタ	電源を接続します。
③	RESET スイッチ	先の細いピンなどを使って 6 秒以上押し続けると、POWER ランプ、MOBILE ランプ、VPN ランプともに点滅し、工場出荷時の設定に戻り、再起動します。
④	DIP スイッチ	拡張用
⑤	SIM カード挿入口	RX110 RX130 RX180 標準タイプの SIM カード(25×15mm)を挿入します。 RX160 nanoSIM カード(12.3×8.8mm)を挿入します。
⑥	保護カバーネジ	DIP スイッチ（④）、SIM カード挿入口（⑤）の使用時には、このネジを外して保護カバーを取り外してください。
⑦	POWER ランプ	Rooster RX の通電状態が表示されます。
⑧	VPN ランプ	VPN セッション（IPsec、PPTP）の動作状態が表示されます。
⑨	MOBILE ランプ	モバイル通信端末の動作状態が表示されます。
⑩	ANT ランプ	電波状態を表示します。
⑪	LAN ランプ	LAN ポート（⑮）への LAN 接続機器の接続状態が表示されます。
⑫	WAN ランプ	WAN/LAN ポート（⑯）への WAN/LAN 接続機器の接続状態が表示されます。
⑬	MOBILE1 コネクタ（SMA）	モバイル通信アンテナを接続します。
⑭	MOBILE2 コネクタ（SMA）	モバイル通信アンテナを接続します。
⑮	LAN1 ポート	LAN ケーブルで LAN 接続機器やハブなどを接続します。
⑯	WAN/LAN2 ポート	LAN ケーブルで WAN 接続機器や LAN 接続機器､ハブなどを接続します。

➲ それぞれのランプの状態は、『1-6　ランプの状態と働き』をご覧ください。

➲ 本装置の寸法については『2-2　取り付け例』をご覧ください。

- ①の FG 端子の接続は必須ではありませんが、お客様の使用用途に応じて必要と思われる場合は接続してご利用ください。
- ⑬の表記が“ANTENNA”となっている機種があります。
- 機種によっては、アンテナコネクタ⑭が無い機種もあります。
- ⑮の表記が“LAN”となっている機種があります。
- ⑯の表記が“WAN”となっている機種があります。
- 本装置で通信を行うためにはアンテナを接続する必要があります。本装置に適したアンテナをご使用ください。
- 無線 LAN 対応の機種につきましては、「RoosterRX 取扱説明書（無線 LAN 版）」をご覧ください。

1-6 ランプの状態と働き

ランプ状態説明

ランプ状態	補足
消灯	
点灯	
点滅	点灯と消灯を繰り返す状態です。
早い点滅	点滅より速く点灯と消灯を繰り返す状態です。
遅い点滅	消灯状態から 4 秒に 1 回点滅します。
2 回点滅	2 回素早く点滅後に消灯を繰り返す状態です。

ランプ点灯・点滅パターン一覧

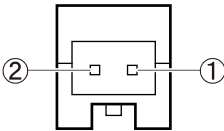
名称	ランプ状態	状態
POWER	点灯	電源が入っていて、使用可能な状態です。
	点滅	起動中、またはおやすみモードへの移行中です。
	遅い点滅	おやすみモード中です。
	消灯	電源が入っていません。
VPN	早い点滅	VPN 接続が確立され、データ通信が行われている状態です。
	点灯	VPN 接続が確立された状態です。
	消灯	VPN 接続が行われていません。
MOBILE	早い点滅	ダイヤルアップ接続で、データ通信が行われている状態です。
	点滅	電話を掛けている状態です。
	2 回点滅	OTASP/OTAPA 中です。 RX160
	点灯	ダイヤルアップ接続が確立された状態です。
	消灯	ダイヤルアップ接続が行われていません。
ANT	点灯	モバイル通信圏内（電波強度：強）
	2 回点滅	モバイル通信圏内（電波強度：やや弱い）
	点滅	モバイル通信圏内（電波強度：弱）
	消灯	モバイル通信圏外
LAN・WAN（緑）	早い点滅	データが流れています。
	点灯	リンクしています。
	消灯	リンクしていません。
LAN・WAN（黄）	点灯	100BASE-T でリンクしています。
	消灯	リンクしていないか、10BASE-T でリンクしています。

1-7 DIPスイッチのパターン

DIP スイッチパターン表

DIP スイッチ				動作モード
1	2	3	4	
OFF	OFF	OFF	ON	Reserved
			OFF	通常モードで動作（工場出荷状態）

- DIP スイッチの変更は、電源が OFF の状態で行ってください。
- DIP スイッチ 1、2、3 は、工場出荷状態（1 : OFF、2 : OFF、3 : OFF）の設定から変更しないでください。変更した場合、正常に動作しません。誤って変更してしまった場合は、必ず DIP スイッチを工場出荷状態に戻してください。

1-8 電源コネクタ

No.	名称	備考
①	VCC	DC5～24V
②	SG	接地

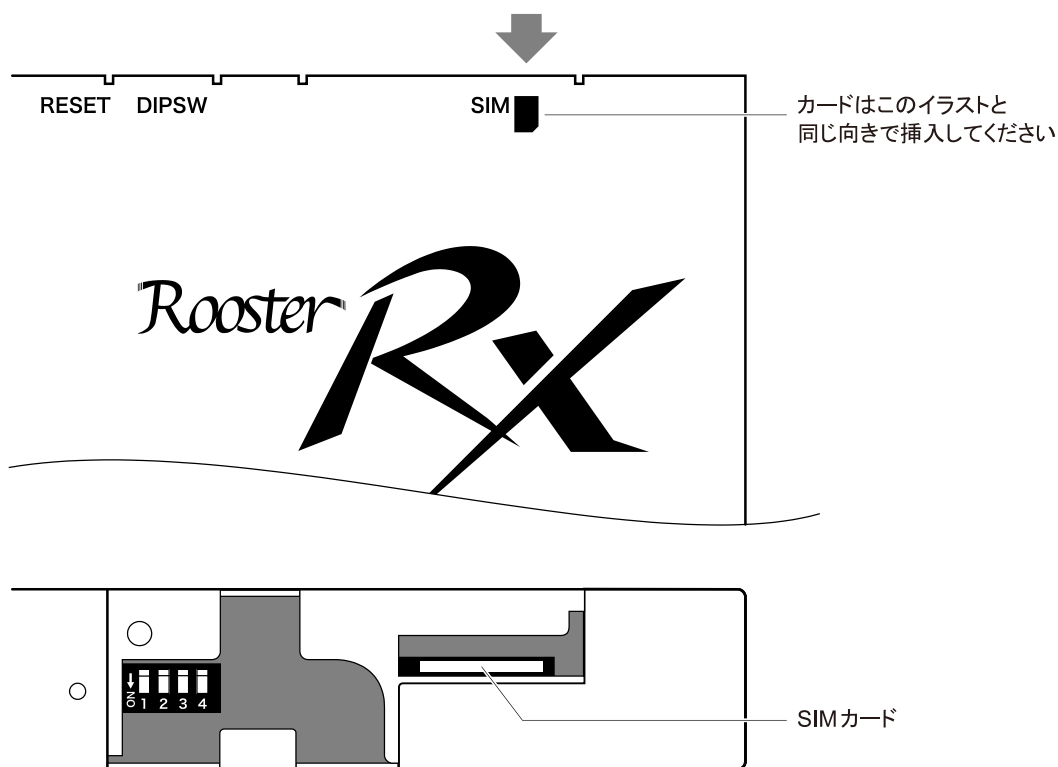
電源仕様

電圧	4.75～29.0V
電流	1A 以上（5V 時）
電圧リップル	100mVp-p 以下
電源コード	電流容量　2A 以上
コネクタ	本体側のコネクタ　JST　S02B-PASK-2 電源コード側のコネクタ　ハウジング　JST　PAP-02V-S コンタクト　JST　SPHD-001T-P0.5 SPHD-002T-P0.5

使用される電源はあらかじめ動作確認の上ご使用ください。

2章　Rooster RXの導入

この章では、Rooster RX の設置方法や接続方法、初期設定について説明します。

2-1 SIMカードの挿入方法

1. Rooster RX 本体側面のネジを外します。

➲ ネジについては『1-5　各部の名称と機能』をご確認ください。

2. SIM カードを挿入します。本体に表示されているイラストと同じ向きで「カチッ」と音がし、ロックされるまで挿入してください。

KDDI との回線契約によっては SIM カードが不要な場合があります。　RX160

2-2 取り付け例(オプションの取り付け金具を使用した場合)

1. 直径 3.5mm の取り付け穴を 137mm の間隔で、2 箇所開け、お客様でご用意いただいたネジで本装置を固定します。

   ▶ 取り付け場所は、平滑な場所をお選びください。

[品番：1P355-RRX-M041]

2. アンテナをアンテナコネクタに接続します。

- 設置場所は平滑な場所をお選びください。また、本製品設置後、ケーブルの抜き差しが十分行えるようなスペースがある場所をお選びください。
- ケーブル類の引きまわしはコネクタに無理な力がかからないように余裕を持たせてください。
- ケーブル類を伝わる水滴が、本製品に侵入しないように、コネクタ近くで一旦コネクタより下方にケーブル類を引きまわしてください。
- 接続するアンテナは、本製品に適合したアンテナをご使用ください。
- この時アンテナの接続には無理な力が加わることのないようにご注意ください。
  (締め付けトルク値 0.9(N・m)で取り付けてください。)
- 適合したアンテナについては弊社までお問い合わせください。
- SIM カード挿入口を下向きに設置しないでください。

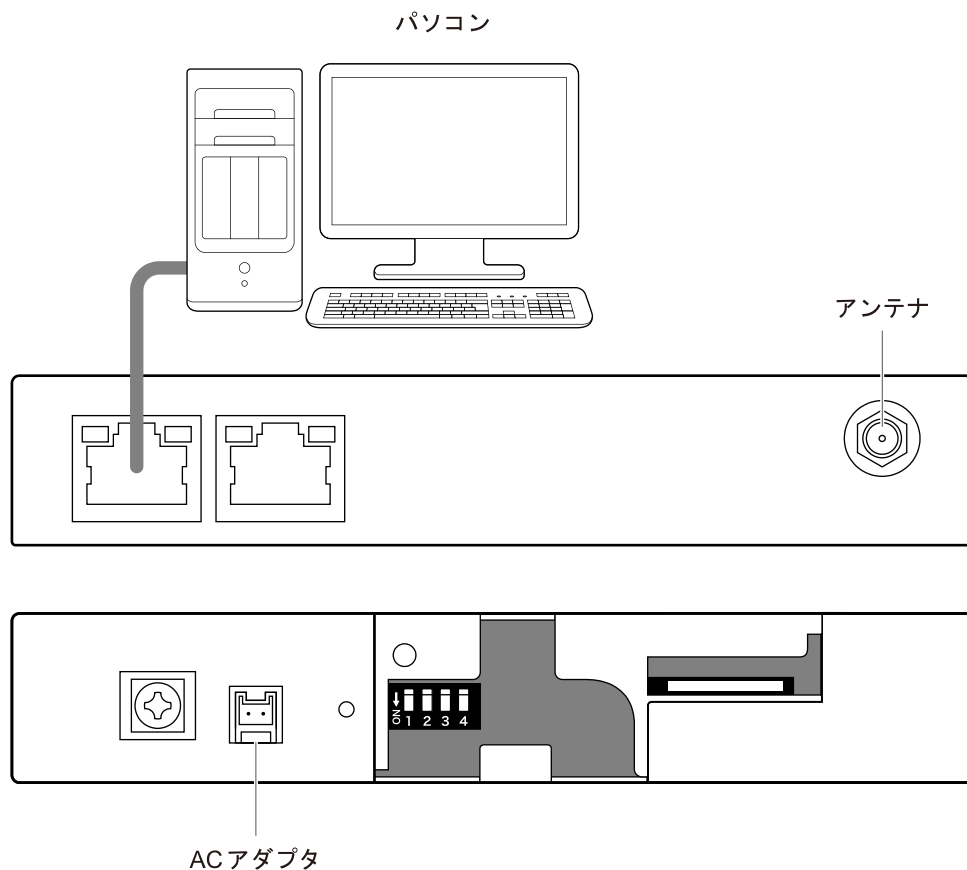
2-3 Rooster RXの接続方法

Rooster RX の設定画面へのアクセスは LAN ポートからのみとなります。設定を行う場合は、パソコンをご用意ください。

2-3-1　必要な環境

- TCP/IP が利用できる OS（Windows、MacOS、各種 UNIX など）を搭載し、イーサネットポートを搭載したパソコン
- LAN ケーブル
- Internet Explorer 10.0 以上のブラウザ

▶ 上記以外のブラウザでは、正常に動作しない可能性があります。

2-3-2　接続方法

1. Rooster RX とパソコンの電源が入っていないことを確認してください。
2. LAN ポートにクライアントとなるパソコンを接続してください。
3. アンテナをアンテナコネクタに接続します。
4. Rooster RX の電源コネクタに AC アダプタを接続してください。次に AC アダプタをコンセントに接続してください。
5. パソコンの電源を入れてください。

- AC アダプタは指定のもの、または規格に合った電源を使用してください。それ以外の電源を使用すると、故障・誤作動の原因になります。その場合の故障は、保証対象外となりますのでご了承願います。
- LAN ケーブルは通信速度に対応したカテゴリのケーブルをご利用ください。

2-4 設置上のご注意

- 設置場所は、平滑な場所をお選びください。また、本装置設置後、コネクタの抜き差しが十分行えるようなスペースがある場所をお選びください。
- ケーブル類の引きまわしは、コネクタに無理な力がかからないように余裕を持たせてください。
- ケーブル類を伝わる水滴が本装置内部に侵入しないように、コネクタ近くで一旦コネクタより下方にケーブル類を引きまわしてください。
- 本装置は雷サージ対策を行っていません。LAN を介して接続されている外部装置側や電源装置で対策を行ってください。

2-5 ご利用環境の確認

Rooster RX とパソコンを接続するためにはパソコンに LAN 環境が必要です。

LAN 環境がない場合には、ご利用のパソコンにあわせて LAN 機器をご用意ください。

- パソコンで LAN ポートが標準で装備されていない場合、LAN アダプタをご利用のパソコンにあわせて増設してください。

通信事業者と、必要に応じてプロバイダとの契約が完了している必要があります。

以下についてご確認願います。

- 3G/4G 回線を利用した回線事業者との契約が完了している必要があります。
- インターネット接続サービスであるプロバイダへの契約が完了している必要があります。（moperaU、softbank 等）

  事業者によっては回線事業者とプロバイダが同じ契約の場合があります。

  その場合別途プロバイダへの契約は必要ありません。
- Rooster RX の設定には、以下の情報が必要になります。回線事業者またはプロバイダとの契約時に提供されている情報をご用意ください。不明な場合はご契約の回線事業者またはプロバイダへお問い合わせください。
  - 接続先名（APN）
  - ユーザー名
  - パスワード
  - ネームサーバ（DNS サーバ）の IP アドレス（設定が必要な場合）

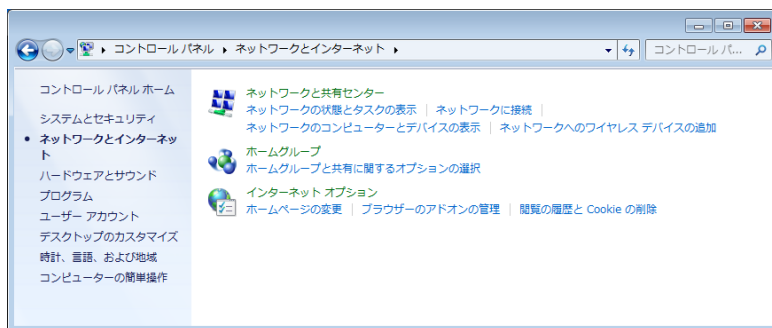
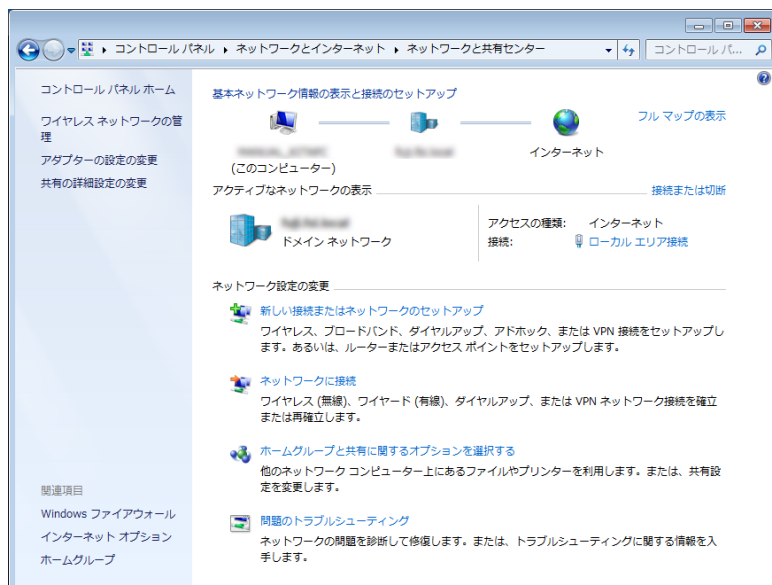
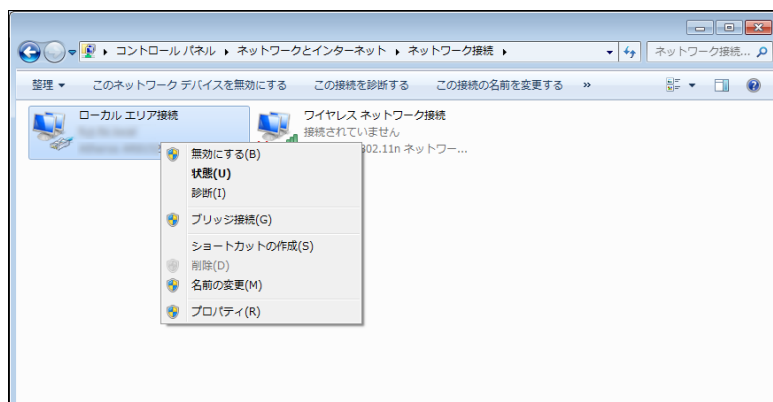
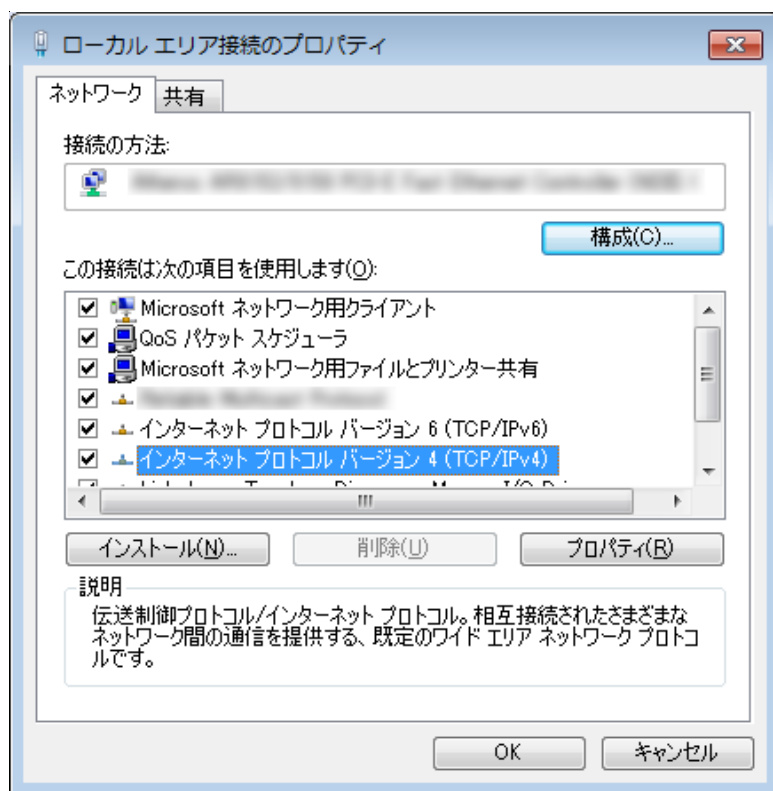
接続先名（APN）は、料金コースによって異なりますので、お間違えのないように十分ご注意ください。

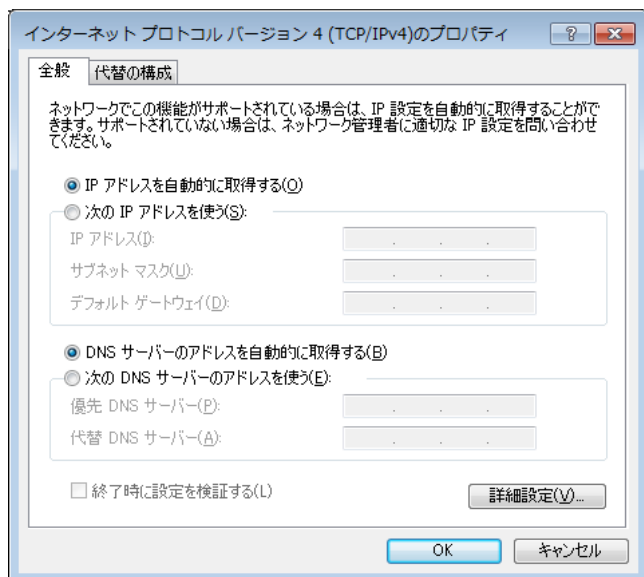
2-6 パソコンの設定

Rooster RX にアクセスできるように、クライアントパソコンに DHCP クライアントの設定をします。DHCP を使用しない場合は、各パソコンに手動で IP を設定する必要があります。その設定方法については、ネットワークカードおよび Windows のマニュアル等をご覧ください。

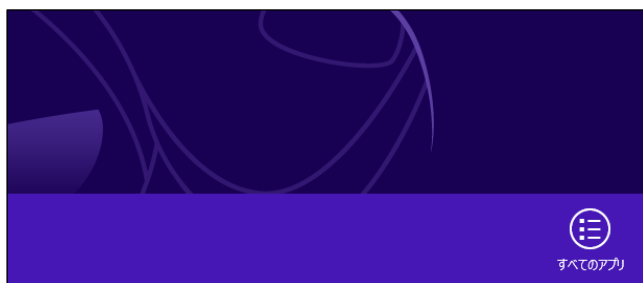
2-6-1 Windows 7の場合

1. パソコンには管理者権限でログインしてください。

2. コントロールパネルから「ネットワークとインターネット」を開きます。

3. 「ネットワークと共有センター」を開きます。

4. 「アダプターの設定の変更」を開きます。

5. ［ローカルエリア接続］を右クリックし、［プロパティ］をクリックします。ローカルエリア接続のプロパティが表示されます。

6. ［インターネットプロトコルバージョン 4（TCP/IPv4）］を選び、［プロパティ］ボタンをクリックします。インターネットプロトコルバージョン 4（TCP/IPv4）のプロパティが表示されます。

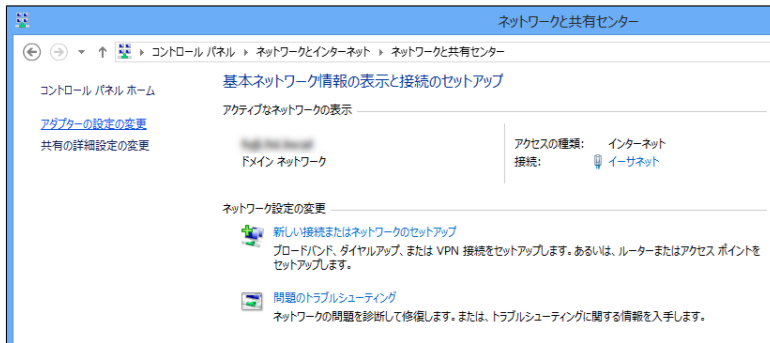
7. ［IP アドレスを自動的に取得する］、［DNS サーバのアドレスを自動的に取得する］を選択します。

8. ［OK］ボタンをクリックしてダイアログを閉じます。
「ローカルエリア接続のプロパティ」画面も、［OK］ボタンをクリックして閉じます。

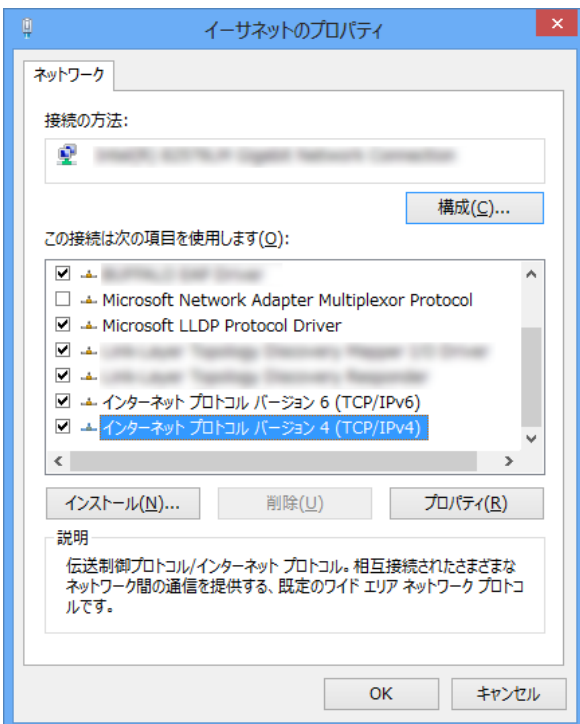
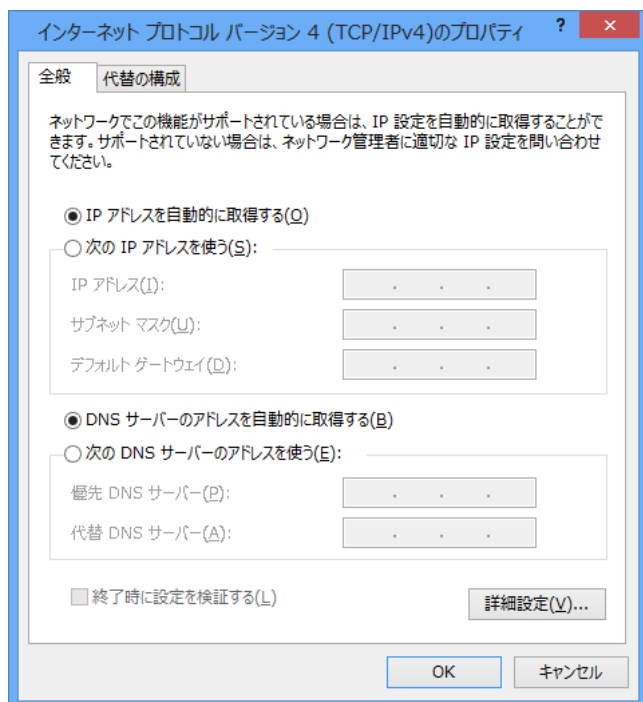
2-6-2　Windows 8の場合

1. パソコンには管理者権限でログインしてください。

2. スタート画面の背景の上で右クリックし、アプリバーから［すべてのアプリ］を開きます。

3. 「コントロールパネル」を開きます。

4. コントロールパネルから「ネットワークとインターネット」を開きます。

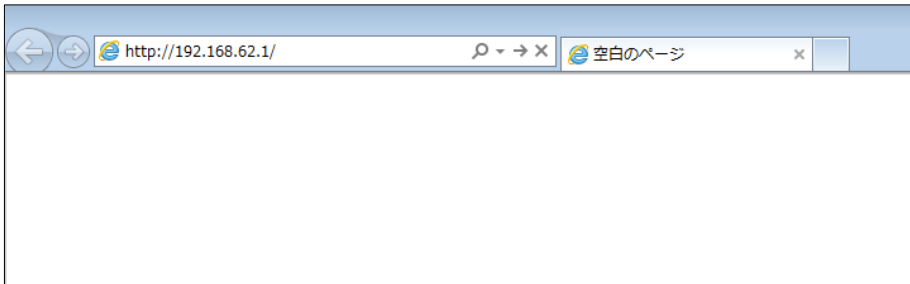
5. 「ネットワークと共有センター」を開きます。

6. 「アダプターの設定の変更」を開きます。

7. ［ローカルエリア接続］を右クリックし、［プロパティ］をクリックします。ローカルエリア接続のプロパティが表示されます。

8. ［インターネットプロトコルバージョン 4（TCP/IPv4）］を選び、［プロパティ］ボタンをクリックします。インターネットプロトコルバージョン 4（TCP/IPv4）のプロパティが表示されます。
9. ［IP アドレスを自動的に取得する］、［DNS サーバのアドレスを自動的に取得する］を選択します。

10. ［OK］ボタンをクリックしてダイアログを閉じます。
「ローカルエリア接続のプロパティ」画面も、［OK］ボタンをクリックして閉じます。

3章　Rooster RXの初期設定

ここでは、パソコンから Rooster RX に接続して、ネットワークやパスワード変更などの初期設定をするまでの手順について説明します。

3-1 Rooster Web設定ツールへのログイン方法

1. WWW ブラウザを起動します。
2. WWW ブラウザのアドレス入力欄に、Rooster RX の LAN 側 IP アドレス「http://192.168.62.1/」（工場出荷時状態）を入力し、Enter キーを押します。

ログインダイアログボックスが表示されます。

3. ユーザー名に「admin」、パスワードに「1234」（工場出荷時状態）と入力した後、［OK］ボタンをクリックします。

4. Rooster RX の設定ツールが表示されます。

- 設定ツールは JavaScript を使用しています。ブラウザの JavaScript をオンにしてから設定を行ってください。
- 設定ツールを表示し、しばらく放置すると、一旦ログアウト処理を行います。その後、設定ツールにアクセスすると、再度ログインダイアログボックスが表示されます。
- ここで入力するユーザー名、パスワードは、Rooster RX の設定ツールにアクセスするためのもので、プロバイダから提供されるユーザー名、パスワードとは異なるものです。

➲ パスワードの変更方法は、『3-3　ログインパスワードの設定』をご覧ください。

3-2 LANの設定

Rooster RX の LAN 側 IP アドレスを変更する場合に設定を行います。

工場出荷時状態の LAN 側 IP アドレスは「192.168.62.1」に設定されています。

1. 設定ツールのメニューから、［インターフェイス］－［LAN］をクリックします。
   「LAN 側設定」のページが表示されます。

2. ［IP アドレス］、［サブネットマスク］に、新しく設定する Rooster RX の LAN 側 IP アドレス、サブネットマスクを入力します。
3. ［設定］ボタンをクリックして、設定を反映させます。

> **!** IP アドレス変更後は、一旦ブラウザを閉じてしばらくお待ちください。その後、新しく設定した IP アドレスで再度設定ツールにログインします。
> なお、変更前と異なるサブネットの IP アドレスに変更した場合、（例.192.168.62.1⇒192.168.0.1 に変更） Rooster RX、パソコン共に再起動を行ってください。

LAN 内の通信状態は、設定ツールのメニューから、［ステータス］－［LAN］をクリックして表示される「LAN ステータス表示画面」から確認することができます。

[LAN/WAN 構成の場合]

[LAN/LAN 構成の場合]

ステータス

現在の設定・状態を表示します。

LAN

■ LAN内の通信状態を表示します。

MACアドレス:		[illegible]
IPアドレス:		192.168.62.1
サブネットマスク:		255.255.255.0
ステータス	LAN1:	接続中
	LAN2:	接続中
送信バイト数:		645124 バイト
送信パケット数:		2251 パケット
送信エラー回数:		0 回
受信バイト数:		263351 バイト
受信パケット数:		2547 パケット
受信エラー回数:		0 回

項目	内容
MAC アドレス	Rooster RX の MAC アドレスが表示されます。
IP アドレス	Rooster RX の IP アドレスが表示されます。
サブネットマスク	Rooster RX のサブネットマスクが表示されます。
[LAN/WAN 構成の場合] ステータス（LAN・WAN） [LAN/LAN 構成の場合] ステータス（LAN1・LAN2）	[LAN/WAN 構成の場合] LAN・WAN ポートへの LAN 接続機器の接続状態が表示されます。 [LAN/LAN 構成の場合] LAN1・LAN2 ポートへの LAN 接続機器の接続状態が表示されます。
送信バイト数	Rooster RX から送信したデータの総バイト数が表示されます。
送信パケット数	Rooster RX から送信したデータの総パケット数が表示されます。
送信エラー回数	Rooster RX からデータ送信を行った際に発生したエラー回数の総計が表示されます。
受信バイト数	Rooster RX で受信したデータの総バイト数が表示されます。
受信パケット数	Rooster RX で受信したデータの総パケット数が表示されます。
受信エラー回数	Rooster RX がデータ受信を行った際に発生したエラー回数の総計が表示されます。

LAN/LAN 構成時の「バイト数/パケット数/エラー回数」は、LAN1/LAN2 を加算した数値になります。（※無線 LAN を使用している場合には、無線 LAN も加算されます。）

3-3 ログインパスワードの設定

ログインパスワードを変更する場合に設定を行います。

工場出荷時状態のパスワードは「1234」に設定されています。

1. 設定ツールのメニューから、［本体設定］－［パスワード変更］をクリックします。
   「パスワードの変更」ページが表示されます。

本体設定

本体の各設定を行います。

パスワード変更

■ ログインパスワードの変更を行います。

古いパスワード：

新しいパスワード：

再入力：

変更

2. ［古いパスワード］に、現在使用しているパスワードを入力します。
3. ［新しいパスワード］に、新しく設定するパスワードを入力します。
4. ［再入力］に、［新しいパスワード］に入力したパスワードを再度入力します。
5. ［設定］ボタンをクリックして、設定を反映させます。
6. ログインダイアログボックスが表示されます。新しく設定したパスワードで再度ログインします。

- 入力したパスワードはすべて、「●」で表示されます。
- 入力可能な文字数は、半角英数字、記号で 16 文字までです。
- ユーザー名の変更はできません。「admin」のみとなります。

3-4 時刻の設定

ここで設定される時刻は、Rooster RX のログ表示などに使用されます。

ログ表示の詳細は、『9 章　ログの参照方法』をご覧ください。

1. 設定ツールのメニューから、［本体設定］－［時刻設定］をクリックします。

   「時刻設定」ページが表示されます。

3-4-1　通信モジュールから取得する場合

1. ［通信モジュールから取得する］チェックをオンにします。
2. ［設定］ボタンをクリックします。

   通信モジュールから取得した時刻に調整されます。

3-4-2　NTPサーバを使用して定期的に時刻を同期する場合

この機能を使用するには、インターネットに接続している必要があります。

➲ インターネット接続設定の詳細は、『4-3　ダイヤルアップ接続設定』をご覧ください。

1. ［NTP サーバ機能を使用する］チェックをオンにし、以下の設定を行います。

項目	内容
NTP サーバ名 1	時刻を問い合わせる NTP サーバアドレス 1 を入力します。
NTP サーバ名 2	時刻を問い合わせる NTP サーバアドレス 2 を入力します。
問合せ間隔	指定された間隔でサーバに NTP サーバに接続し､時刻を同期します。 「0」を設定した場合、Rooster RX の起動後、1 回のみ同期します。

2. ［設定］ボタンをクリックして、設定を反映させます。
設定完了後、［今すぐ問合せを行う］ボタンをクリックすると、設定した NTP サーバに接続して時刻を同期します。

NTP の問い合わせに失敗した場合は､成功するまで約 5 分間隔で問い合わせを実行します。

時刻同期を行う際､WAN 回線が接続されていない場合､モバイル通信端末の設定によっては自動的にダイヤルを行います。

➲『4-3　ダイヤルアップ接続設定』をご覧ください。

3-4-3　手動で時刻の設定を行う場合

1. ［手動設定］の各欄に、現在の時刻を入力します。
2. ［手動設定］ボタンをクリックします。

直ちに設定した時刻に調整されます。

3-5 メールアカウントの設定

ここで設定されるメールアカウントは、Rooster RX の、メール送信によるアドレス解決機能に使用されます。メール送信によるアドレス解決機能を使用する必要がない場合、メールアカウントの設定の必要はありません。

➔ アドレス解決機能の詳細は、『7-1 アドレス解決機能』をご覧ください。

1. 設定ツールのメニューから、［本体設定］－［メールアカウント設定］をクリックします。

   「メールアカウントの設定」ページが表示されます。

本体設定

本体の各設定を行います。

メールアカウント設定

■ 各種サービスを利用するためのメールアカウント設定を行います。

サービスの種類: POP Before SMTP

SMTPサーバ名: smtp.mailserver.com

SMTPポート番号: 25

POP3サーバ名: pop.mailserver.com

アカウント: suncomm

パスワード: •••••••

設定

2. 以下の設定を行います。

項目	内容
サービスの種類	メールサーバの種類を選択します。「POP Before SMTP」、「ユーザ認証 SMTP」のいずれかを選んでください。
SMTP サーバ名	送信メールサーバ名を設定します。
SMTP ポート番号	送信ポート番号を設定します。
POP3 サーバ名	受信メールサーバ名を設定します。
アカウント	アカウント名を設定します。
パスワード	使用するメールアカウントのパスワードを入力します。

上記の設定で不明な部分につきましては、インターネットプロバイダ、あるいはサーバ管理者までお問い合わせください。

3. ［設定］ボタンをクリックして、設定を反映させます。

3-6 おやすみモードの設定

Rooster RX の省電力の制御を行います。この機能は定期的に Rooster RX をサスペンド（消費電力を抑えた待機状態）することにより、電力の消費を抑えることができます。

1. 設定ツールのメニューから、［本体設定］－［おやすみモード］をクリックします。

   「おやすみモードの設定」ページが表示されます。

2. ［おやすみモードを使用する］チェックをオンにし、以下の設定を行います。

項目	内容
指定待機時間経過によるサスペンドを使用する	待機時間が経過したら常にサスペンド状態にする場合に選択します。また、以下の設定を行ってください。 • サスペンドまでの待機時間設定 サスペンドまでの待機時間を入力します。
指定スケジュールによるサスペンドを使用する	スケジュールを指定しておやすみモードの管理をする場合に選択します。また、以下の設定を行ってください。 • スケジュールリストの設定 クリックすると、「おやすみモードのスケジュール設定」ページが表示されます。おやすみモードのスケジュールを設定します。 • サスペンドまでの待機時間設定 サスペンド期間中にレジューム（サスペンドから復帰している状態）した場合にサスペンドまでの待機時間を入力します。

3. ［設定］ボタンをクリックして、設定を反映させます。
［指定スケジュールによるサスペンドを使用する］を選択した場合、［スケジュールリストの設定］をクリックすると、「おやすみモードのスケジュール設定」ページが表示されます。

4. 新しくスケジュールの登録を行う場合は、［追加］ボタンをクリックします。設定済みのスケジュールを変更する場合は、［変更］をクリックします。
5. ［追加］ボタン、または［変更］をクリックすると、「おやすみモードのスケジュール詳細設定」ページが表示されます。［追加］ボタンをクリックした場合は空白の状態で、［変更］をクリックした場合は、表示されているスケジュール設定の変更が行えます。［削除］をクリックすると、表示されているスケジュール設定が削除されます。［戻る］ボタンをクリックすると、「おやすみモードの設定」ページに戻ります。

memo 設定可能なスケジュールの設定は 7 件まで行えます。

6. 以下の設定を行います。

項目	内容
No	おやすみモードスケジュール設定の通し番号が表示されます。
サスペンド曜日	サスペンドさせたい曜日を選択します。
サスペンド時刻	サスペンドさせたい時刻を設定します。
レジューム曜日	レジュームさせたい曜日を選択します。
レジューム時刻	レジュームさせたい時刻を設定します。

7. ［追加］ボタンをクリックして設定内容を反映させます。［キャンセル］ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「おやすみモードのスケジュール設定」ページに戻ります。

3-6-1　おやすみモード設定例

条件

以下の条件でおやすみモードを設定する場合の例について説明します。

- 月曜日から金曜日まで PM9:00～AM8:00 まで省電力で使用する。
- 土曜日、日曜日は全日省電力で使用する。
- サスペンド期間中にレジュームした場合の再サスペンドまでの待機時間を 10 分とする。

設定

1　「おやすみモードの設定」ページで以下の設定を行います。

- ［おやすみモード機能を使用する］にチェックを入れます。
- ［指定スケジュールによるサスペンドを使用する］を選択します。
- ［サスペンドまでの待機時間設定］に「10」と入力します。
- ［設定］ボタンを押下します。

2　［スケジュールリストの設定］をクリックします。

「スケジュール設定」ページが表示されます。

3 「スケジュール設定」ページで［追加］ボタンをクリックし、［サスペンド曜日］、［サスペンド時刻］、［レジューム曜日］、［レジューム時刻］を下図のように設定します。

本体設定

本体の各設定を行います。

おやすみモード

■ おやすみモードのスケジュール設定を行います。

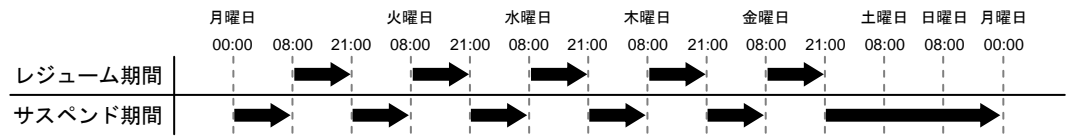
設定の追加 追加

No.	サスペンド曜日	サスペンド時刻	レジューム曜日	レジューム時刻	操作
1	月曜日	21:00	火曜日	08:00	変更 削除
2	火曜日	21:00	水曜日	08:00	変更 削除
3	水曜日	21:00	木曜日	08:00	変更 削除
4	木曜日	21:00	金曜日	08:00	変更 削除
5	金曜日	21:00	月曜日	08:00	変更 削除

戻る

以上で、条件が設定されました。

おやすみモード設定例の状態遷移

上記の設定によるおやすみモードの状態遷移は次のようになります。

memo

サスペンド期間中に着信などでレジュームした場合は、10 分の待機時間の後、再度サスペンド状態となります。
レジューム期間中に待機時間が 10 分経過した場合は、サスペンド状態とはなりません。

3-7 電源制御

Rooster RX の電源の制御を行います。この機能は定期的に Rooster RX の電源を ON/OFF することにより、より安定した運用を行うことを目的とします。

1. 設定ツールのメニューから、［本体設定］－［電源制御］をクリックします。
   「電源制御」のページが表示されます。

本体設定

本体の各設定を行います。

電源制御

■ 自動電源ON/OFFの設定を行います。

□ ハードウェアの自動電源ON/OFF機能を使用する。
間隔： 1日

□ ソフトウェアの自動電源ON/OFF機能を使用する。
動作条件： ◉ 回線接続中は電源ON/OFFしない。
○ 回線接続中でも電源ON/OFFする。

◉ 間隔指定
間隔： 1日

○ 時刻指定
00 時 00 分 (00:00～23:59)

◉ 毎日
○ 曜日指定
□ :月 □ :火 □ :水 □ :木
□ :金 □ :土 □ :日

設定

2. 以下の設定を行います。

<table>
<tr><th>項目</th><th>内容</th></tr>
<tr><td>ハードウェア</td><td>ハードウェアの電源を ON/OFF するための設定です。
使用する場合はチェックをオンにし、以下の設定を行ってください。
▶ ソフトウェアの設定が何らかの影響にて動作しなかった時の保険的な機能です。
• 間隔指定
間隔を 1〜7 日の間で設定します。
<例>
ハードウェア：1 日間隔

回線がつながっていても 24 時間ごとに再起動します。
回線がつながっている状態でも、設定時間になるとハードウェアが再起動します。ソフトウェアの設定が何らかの影響にて動作しなかった時の保険的な機能です。
ハードウェアの設定時間は目安ですので、実際の動作時間は多少前後します。</td></tr>
<tr><td>ソフトウェア</td><td>ソフトウェア上で Rooster RX の電源を ON/OFF するための設定です。
使用する場合はチェックをオンにし、以下の設定を行ってください。
• 動作条件
回線接続中の際に電源を ON/OFF するか否かを選択します。
• 間隔指定
ソフトウェアにおいて、日にち間隔で設定する場合はチェックをオンにし、間隔を 1〜7 日の間で設定します。
• 時刻指定
再起動させたい時刻を指定します。24 時間表記にて設定します。またその曜日を「毎日」または「曜日指定」にて設定します。
<例>
ソフトウェア：使用する、回線接続中は電源 ON/OFF しない、1 日ごと

設定時間の 24 時間を経過しても、回線がつながっている状態では再起動しません。回線が切断された時に再起動します。
「回線接続中でも電源 ON/OFF する」を選択した場合、設定時間がきたら通信を行っている場合でも強制的に再起動をします。</td></tr>
</table>

3. 選択した設定でよければ［設定］ボタンをクリックします。
4. 設定を反映させるためには、Rooster RX を再起動させる必要があります。

内蔵のモバイル通信端末については、独自に 24 時間ごとにリセットする機能が搭載されています（工場出荷時の設定）。回線がつながっている状態ではモバイル通信端末は再起動せず、回線切断後に再起動します。

3-8 WANの設定

Rooster RX の WAN 側のネットワーク設定を行います。

1. 設定ツールのメニューから、［インターフェイス］－［WAN］をクリックします。
   「WAN 側設定」のページが表示されます。

2. 以下の設定を行います。

項目	内容
IP 自動取得	WAN 側の IP を自動で取得する場合は、チェックをオンにします。
IP 手動設定	WAN 側の IP を手動で設定する場合は、チェックをオンにします。
PPPoE 接続	PPPoE 接続を行う場合は、チェックをオンにします。
LAN として使用	WAN ポートを LAN として使用（LAN/LAN 構成として使用）する場合は、チェックをオンにします。
IP アドレス	IP 手動設定を選択した場合は、WAN 側の IP アドレスを設定します。
サブネットマスク	IP 手動設定を選択した場合は、WAN 側のサブネットマスクを設定します。
デフォルトゲートウェイ	IP 手動設定を選択した場合は、WAN 側のデフォルトゲートウェイを設定します。
DNS サーバ 1	IP 手動設定を選択した場合は、プライマリ DNS サーバを設定します。
DNS サーバ 2	IP 手動設定を選択した場合は、セカンダリ DNS サーバを設定します。
ID	PPPoE 接続を選択した場合は、認証するための ID を設定します。
パスワード	PPPoE 接続を選択した場合は、認証するためのパスワードを設定します。
NAT を使用する。	NAT 機能を使用する場合は、チェックをオンにします。

3. ［設定］ボタンをクリックして、設定を反映させます。

WAN 内の通信状態は、設定ツールのメニューから、［ステータス］－［WAN］をクリックして表示される「WAN/PPPoE ステータス表示画面」から確認することができます。

[LAN/WAN 構成の場合]（IP 自動取得、IP 手動設定、PPPoE 接続を選択）

項目		内容
操作	［接続／切断］ボタン	• WAN 側と切断中は［接続］ボタンが表示されます。WAN 側との通信を接続する場合はクリックします。 • WAN 側と接続中は［切断］ボタンが表示されます。WAN 側との通信を切断する場合はクリックします。 ▶ WAN が無効の状態では操作できません。
	［DHCP 再取得］ボタン	DHCP を再取得します。
	［無効／有効］ボタン	• WAN が有効の場合は［無効］ボタンが表示されます。WAN を無効にする場合はクリックします。 ▶ WAN を無効にすると、接続が切断されます。有効にするまで WAN 接続は行われません。 • WAN が無効の場合は［有効］ボタンが表示されます。WAN を有効にする場合はクリックします。
ステータス		設定した WAN の現在の状態が表示されます。
MAC アドレス		MAC アドレスが表示されます。
IP アドレス		WAN 側の IP アドレスが表示されます。
サブネットマスク		WAN 側のサブネットマスクが表示されます。
デフォルトゲートウェイ		WAN 側のデフォルトゲートウェイが表示されます。
DNS サーバ 1		プライマリ DNS サーバが表示されます。
DNS サーバ 2		セカンダリ DNS サーバが表示されます。
送信バイト数		WAN 側に送信したデータの総バイト数が表示されます。
送信パケット数		WAN 側に送信したデータの総パケット数が表示されます。

項目	内容
送信エラー回数	WAN 側にデータ送信を行った際に発生したエラー回数の総計が表示されます。
受信バイト数	WAN 側から受信したデータの総バイト数が表示されます。
受信パケット数	WAN 側から受信したデータの総パケット数が表示されます。
受信エラー回数	WAN 側からデータ受信を行った際に発生したエラー回数の総計が表示されます。

[LAN/LAN 構成の場合]（LAN として使用を選択）

ステータス

現在の設定・状態を表示します。

WAN／PPPoE

■ WANまたはPPPoE通信の状態を表示します。

ステータス: LANとして使用中

項目	内容
ステータス	設定した WAN の現在の状態が表示されます。 ➲ ステータスの詳細については、『WAN のステータス一覧』をご覧ください。

WAN のステータス一覧

ステータス表示	状態
無効	接続設定が無効になっています。
未接続	接続が切断されている状態です。
接続済	接続が正常に行えた状態です。
LAN として使用中	LAN/LAN 構成で使用中の状態です。

4章　ダイヤルアップ設定

ここでは、ダイヤルアップ接続するために必要な設定を行います。

4-1 APN設定

RX110　RX130

Rooster RX ではインターネット接続を行う場合、最初に APN の設定が必要になります。ご契約のインターネットサービスプロバイダ（以下プロバイダ）等からご提供された情報をご用意ください。

• APN（アクセスポイントネーム）　• ユーザー名　• パスワード

1. 設定ツールのメニューから、［インターフェイス］－［モバイル通信端末］をクリックします。「モバイル通信端末」のページが表示されます。

2. ［APN の設定］をクリックします。「APN の設定」のページが表示されます。

3. 新しく APN の登録を行う場合は、［追加］ボタンをクリックします。設定済みの APN を変更する場合は、［変更］をクリックします。

4. ［追加］ボタン、または［変更］をクリックすると、「APN 設定の詳細設定」ページが表示されます。［追加］ボタンをクリックした場合は空白の状態で、［変更］をクリックした場合は、「APN 設定の詳細設定」ページが表示され、表示されている APN 設定の変更が行えます。［削除］をクリックすると、表示されている接続先設定が削除されます。［戻る］ボタンをクリックすると、「モバイル通信端末設定」のページに戻ります。

- 設定可能な APN の設定は 10 件までです。
- 追加登録時、CID 項目に登録済の cid 番号を入力して登録すると、登録済の cid 番号へ APN 設定が上書きされます。

5. 以下の設定を行います。

項目	内容
CID	登録する cid 番号を入力します。 APN 設定の変更時は入力できません。
APN	ご契約のプロバイダのアクセスポイントネームを入力します。
プロトコル	プロトコルタイプを選択します。 「IP」または「PPP」のいずれかを選択します。
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶ 半角 16 文字（全角 8 文字）までの任意の文字列を入力できます。

6. ［設定］ボタンをクリックして設定内容を反映させます。［キャンセル］ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「APN の設定」のページに戻ります。

APN 設定の初期値

CID	APN	プロトコル	メモ
1	mopera.net	IP	moperaU
5	mopera.flat.foma.ne.jp	IP	moperaU 定額制

RX160

Rooster RX ではインターネット接続を行う場合、最初に APN の設定が必要になります。ご契約のインターネットサービスプロバイダ（以下プロバイダ）等からご提供された情報をご用意ください。

• APN（アクセスポイントネーム）　• ユーザー名　• パスワード

※ただし、『4-3-1　ダイヤルアップ接続先の追加、変更方法』の詳細設定で、「ID」の項目に「@」が含まれる場合これが APN 名として優先され、本設定の設定値は使用されません。

1. 設定ツールのメニューから、［インターフェイス］－［モバイル通信端末］をクリックします。「モバイル通信端末」のページが表示されます。

2. ［APN の設定］をクリックします。「APN の設定」のページが表示されます。

3. 新しく APN の登録を行う場合は、［追加］ボタンをクリックします。設定済みの APN を変更する場合は、［変更］をクリックします。

4. ［追加］ボタン、または［変更］をクリックすると、「APN 設定の詳細設定」ページが表示されます。［追加］ボタンをクリックした場合は空白の状態で、［変更］をクリックした場合は、「APN 設定の詳細設定」ページが表示され、表示されている APN 設定の変更が行えます。［削除］をクリックすると、表示されている接続先設定が削除されます。［戻る］ボタンをクリックすると、「モバイル通信端末設定」のページに戻ります。

• 設定可能な APN の設定は 1 件までです。

APN設定の詳細設定

CID	1
APN	au.au-net.ne.jp
メモ	LTE NET for DAT

設定 キャンセル

5. 以下の設定を行います。

項目	内容
CID	登録する cid 番号を入力します。 APN 設定の変更時は入力できません。
APN	ご契約のプロバイダのアクセスポイントネームを入力します。
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶ 半角 16 文字（全角 8 文字）までの任意の文字列を入力できます。

6. ［設定］ボタンをクリックして設定内容を反映させます。［キャンセル］ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「APN の設定」のページに戻ります。

APN 設定の初期値

CID	APN	メモ
1	au.au-net.ne.jp	LTE NET for DATA

RX180

Rooster RX ではインターネット接続を行う場合、最初に APN の設定が必要になります。ご契約のインターネットサービスプロバイダ（以下プロバイダ）等からご提供された情報をご用意ください。
• APN（アクセスポイントネーム）　• ユーザー名　• パスワード

1. 設定ツールのメニューから、［インターフェイス］－［モバイル通信端末］をクリックします。「モバイル通信端末」のページが表示されます。

2. ［APN の設定］をクリックします。「APN の設定」のページが表示されます。

3. 新しく APN の登録を行う場合は、［追加］ボタンをクリックします。設定済みの APN を変更する場合は、［変更］をクリックします。

4. ［追加］ボタン、または［変更］をクリックすると、「APN 設定の詳細設定」ページが表示されます。［追加］ボタンをクリックした場合は空白の状態で、［変更］をクリックした場合は、「APN 設定の詳細設定」ページが表示され、表示されている APN 設定の変更が行えます。［削除］をクリックすると、表示されている接続先設定が削除されます。［戻る］ボタンをクリックすると、「モバイル通信端末設定」のページに戻ります。

- 設定可能な APN の設定は 10 件までです。
- 追加登録時、CID 項目に登録済の cid 番号を入力して登録すると、登録済の cid 番号へ APN 設定が上書きされます。

5. 以下の設定を行います。

項目	内容
CID	登録する cid 番号を入力します。 APN 設定の変更時は入力できません。
APN	ご契約のプロバイダのアクセスポイントネームを入力します。
プロトコル	プロトコルタイプを選択します。 「IP」のみの設定となります。
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶ 半角 16 文字（全角 8 文字）までの任意の文字列を入力できます。

6. ［設定］ボタンをクリックして設定内容を反映させます。［キャンセル］ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「APN の設定」のページに戻ります。

APN 設定の初期値

CID	APN	プロトコル	メモ
1	softbank	IP	SoftBank
2	bizflat.softbank	IP	ULTRA SPEED

RAS 着信を使用する場合は、CID1 に RAS 着信を行う APN を設定してください。

4-2 OTA RX160

Rooster RX160 では、OTA システムにより利用開始登録や解約を行います。
OTA システムとは、モバイル無線通信を利用して電話番号や ID の書き込み・消去を可能にする機能です。

4-2-1 OTASP（利用開始登録）

通信モジュールを使用できる状態にするには、OTASP（利用開始登録）を行います。

【OTASP の流れ】

1. OTASP を行うには事前に KDDI への申込みを行ってください。

↓

2. KDDI より実施時期の連絡があります。

↓

3. RoosterRX で OTASP 操作を行います。

※OTASP 操作は、モバイル通信端末ステータス画面『4-4 接続／切断方法』から行います。
OTASP 操作が必要な場合には、モバイル通信端末ステータス画面の「操作」の項目に「OTASP」と表示されますので、それをクリックします。OTASP が完了して通信モジュールが使用可能状態になると、「ステータス」の項目が「待受中」と表示されます。

・OTASP は通信モジュールのステータスが「未登録」の場合にのみ行えます。
・OTASP を行うにはモバイル通信端末の設定を有効にしてください。
（『4-3　ダイヤルアップ接続設定』もしくは『5-1　RAS 着信接続設定』、『5-2　WakeOn 着信の設定』のいずれかを有効にしてください）
・OTASP は起動直後に行ってください。OTASP に失敗する場合があります。
OTASP に失敗した場合は、再度 OTASP 操作を行ってください。
・電波状態が良好な場所で行ってください。

➲ モバイル通信端末ステータス画面の詳細は、『4-4　接続／切断方法』をご覧ください。

4-2-2 OTAPA（利用解約）

【OTAPA の流れ】

1. 通信モジュールを解約状態にするには、KDDI への申込みを行ってください。

↓

2. KDDI より実施時期の連絡があります。

↓

3. 実施時期に RoosterRX の電源を入れておきます。

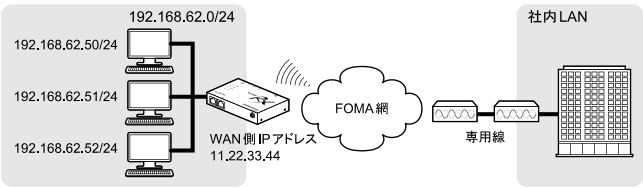
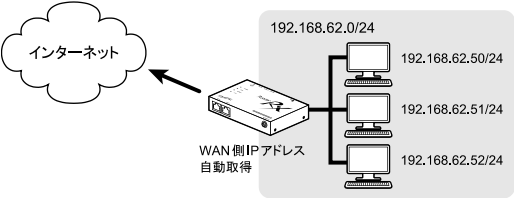
・KDDI への解約申込みを行ったにも関わらず OTAPA を行わない場合、以降通信モジュールが使用できなくなる為、OTAPA は必ず行ってください。
・OTAPA は通信網側から行われるため、RoosterRX からの操作では行えません。
・KDDI へ申込みを行った OTAPA をする時間は RoosterRX の電源を入れた状態で、通信モジュールのステータスを「待受中」にしてください。
・回線接続中に OTAPA が行われた場合、回線接続状態のまま通信できなくなり、OTAPA が行われたログが残りませんのでお気をつけください。
・電波状態が良好な場所で行ってください。

4-3 ダイヤルアップ接続設定

1. 設定ツールのメニューから、［インターフェイス］－［モバイル通信端末］－［ダイヤルアップ］ をクリックします。

   「ダイヤルアップ接続設定」のページが表示されます。

2. ［ダイヤルアップ接続を行う］のチェックをオンにし、以下の設定を行います。

項目	内容
ダイヤルアップ先の設定	クリックすると、モバイル通信端末によるダイヤルアップ接続先の表示、追加が行えます。 ➲ 設定方法は、『4-3-1　ダイヤルアップ接続先の追加、変更方法』をご覧ください。
ダイヤルアップモードの設定	RX110　RX130 ダイヤルアップのモードを選択します。 ［通常］または［ビジネス mopera］のいずれかを選択します。 • モードが「通常」の場合 インターネットへ接続される場合には［通常］を選択ください。 WAN 側の IP アドレスが固定の場合には［本体側 IP アドレス］に、指定の IP アドレスを入力してください。

項目	内容
	• モードが「ビジネス mopera」の場合 192.168.62.0/24 192.168.62.50/24 192.168.62.51/24 192.168.62.52/24 WAN側IPアドレス 11.22.33.44 FOMA網 専用線 社内LAN ▶NTT ドコモのビジネス mopera アクセスプレミアム／アクセスプロをご利用の際には、［ビジネス mopera］を選択ください。 NTT ドコモとの契約が必要になります。 ビジネス mopera アクセスプレミアム／アクセスプロにつきましては、NTT ドコモのホームページをご覧ください。 RX160 RX180 ダイヤルアップのモードを選択します。 ［通常］を選択します。 インターネット 192.168.62.0/24 192.168.62.50/24 192.168.62.51/24 192.168.62.52/24 WAN側IPアドレス 自動取得 WAN 側の IP アドレスが固定の場合には［本体側 IP アドレス］に、指定の指定の IP アドレスを入力してください。
自動接続を行う	チェックをオンにすると、LAN 側から発信要求があった場合、もしくは Rooster RX の各種サービスによる接続要求があった場合等に、自動発信が行われるようになります。セッションキープの設定は、自動接続の設定をオンにするとできるようになります。 チェックをオフにすると、接続、切断の動作は設定ツールのみで行うようになります。
セッションキープを行う	回線接続を維持させておきたい時にチェックをオンにします。 従量制課金でご契約の場合は、設定しないようにしてください。意図しない接続で通信料金が掛かってしまう原因となりますので、くれぐれもご注意願います。
LCP Echo Request による接続監視を行う	チェックをオンにすると、LCP Echo Request を送信します。 送信間隔、切断動作をさせる回数を設定します。
無通信監視を行う	チェックをオンにすると、Rooster RX に指定した秒数の間、通信が行われなかった時、自動的に回線を切断するようになります。 チェックがオンになっていても、「0」を入力した場合、無通信監視は行いません。 従量制課金でご契約の場合は、必ず設定するようにしてください。
NAT を使用する	WAN 側への通信を行う際に IP アドレスの変換が必要になる場合、チェックをオンにします。インターネット接続を行う場合、通常はチェックをオンにしてください。
本体側 IP アドレス：自動取得	WAN 側の IP アドレスが自動取得の場合はこちらを選択します。
本体側 IP アドレス：IP 固定	WAN 側の IP アドレスが固定の場合はこちらを選択します。
IP アドレス	本体側 IP アドレスを［IP 固定］で選択した際には、IP アドレスを入力します。
認証プロトコル	［PAP］、［CHAP］、［相手に合わせる］のいずれかを選択します。

3. ［設定］ボタンをクリックして、設定内容を反映させます。

［ダイヤルアップ先の設定］を行う前に、ここで一度、［設定］ボタンをクリックして、設定内容を反映させます。［ダイヤルアップ先の設定］を先にクリックすると、設定した内容が破棄されてしまいます。

4-3-1　ダイヤルアップ接続先の追加、変更方法

1. ［ダイヤルアップ先の設定］をクリックします。

「ダイヤルアップ接続先リスト」のページが表示されます。

まだダイヤルアップ接続先を追加していない場合

すでにダイヤルアップ接続先を追加している場合

2. 新しく接続先の登録を行う場合は、［追加］ボタンをクリックします。設定済みのダイヤルアップ接続先を変更する場合は、［変更］をクリックします。

3. ［追加］ボタン、または［変更］をクリックすると、「ダイヤルアップ接続先の詳細設定」ページが表示されます。［追加］ボタンをクリックした場合は空白の状態で、［変更］をクリックした場合は、「ダイヤルアップ接続先の詳細設定」ページが表示され、表示されている接続先設定の変更が行えます。［削除］をクリックすると、表示されている接続先設定が削除されます。［戻る］ボタンをクリックすると、「ダイヤルアップ接続設定画面」のページに戻ります。

memo

ダイヤルアップ接続先の設定は最大 8 件まで行えます。

ダイヤルアップ接続先の詳細設定

No.	1
宛先IPアドレス	10.11.12.0
宛先ネットマスク	255.255.255.0
電話番号	*99***1#
ID	suncomm
パスワード	●●●●●●●
接続方式	通常ダイヤルアップ
本体側IPアドレス	0.0.0.0
メモ	

設定　キャンセル

4. 以下の設定を行います。

項目	内容
宛先 IP アドレス	接続先ネットワークの IP アドレス（例. 10.11.12.0） （空欄：全パケットが対象となります。最初に空欄があった場合全てその項目を用いてダイヤルアップします。）
宛先ネットマスク	接続先のネットワークのサブネットマスク（例. 255.255.255.0)
電話番号	RX110 RX130 RX180 アクセスポイントへの電話番号を以下の形式で入力します。 「＊99＊＊＊●#」 ▶ ●の部分には、APN の設定で設定した cid 番号を入力します。 ➲ 設定方法は、『4-1 APN 設定』をご覧ください。 ❗ 誤った cid 番号を設定しますと意図しない接続で通信料金が掛かってしまう原因となりますので、くれぐれもご注意願います。 RX160 アクセスポイントへの電話番号を以下の形式で入力します。 「＊99」 ➲ 接続するアクセスポイントへの APN 設定が必要な場合があります。必要な場合『4-1 APN 設定』をご覧ください。
ID	RX110 RX130 RX180 プロバイダから提供されたユーザー名を入力します。 RX160 ID に『@』が含まれる場合、これが APN 名として優先して設定されます。（この場合、『4-1 APN 設定』の設定値は使用されません。）

項目	内容
パスワード	プロバイダから提供されたパスワードを入力します。 ❗ ID およびパスワードで、下記の文字は設定できません。 # （シャープ）　¥ （円マーク） ' （シングル クォーテーション）　" （ダブル クォーテーション） ` （バック クォーテーション）　␣ （スペース） ( ) （カッコ）　[ ] （大カッコ） ❗ 設定できない文字が含まれている場合は、インターネットサービスプロバイダ、あるいはネットワーク管理者に上記の文字を使用しない ID・パスワードに変更をご依頼ください。
接続方式	［通常ダイヤルアップ］のみの設定となります。
本体側 IP アドレス	WAN 側の IP アドレスを入力します。 （空欄：ダイヤルアップ設定の指定を使用します。 0.0.0.0：自動取得を行います。）
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶半角 16 文字（全角 8 文字）までの任意の文字列を入力できます。

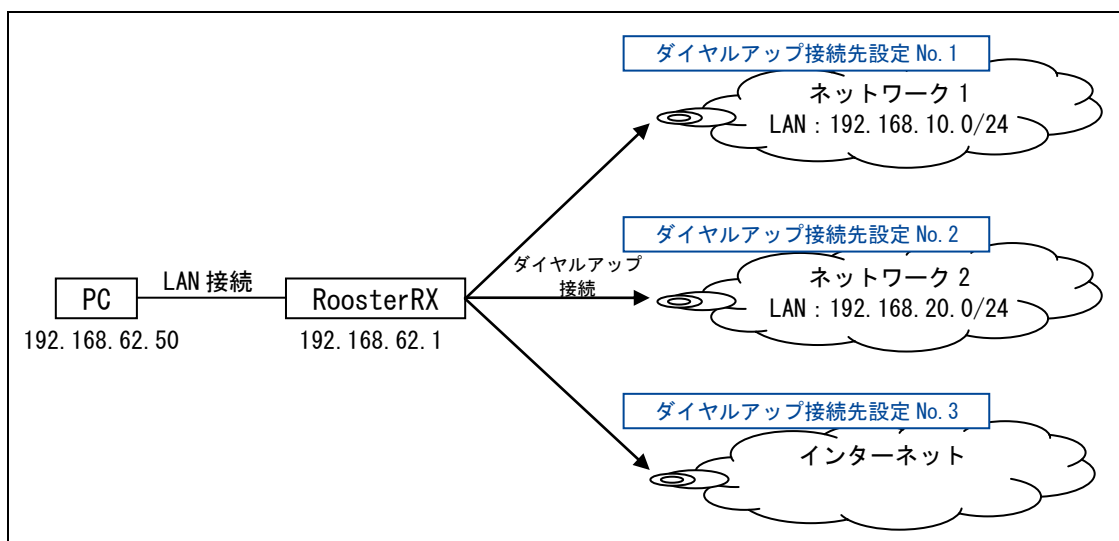
5. ［設定］ボタンをクリックして設定内容を反映させます。［キャンセル］ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「ダイヤルアップ接続先リスト」のページに戻ります。

掛け分けの設定例

ダイヤルアップ接続先を複数設定することで、ダイヤルアップの掛け分けを行うことができます。ここでは掛け分けの設定例を示します。下記のように RoosterRX から 3 か所に掛け分けたい場合、3 つのダイヤルアップ接続先の設定を行います。

「ダイヤルアップ接続先設定 No.1」は、192.168.10.0/24 のプライベートネットワークを持つ「ネットワーク 1」へのダイヤルアップ設定。

「ダイヤルアップ接続先設定 No.2」は、192.168.20.0/24 のプライベートネットワークを持つ「ネットワーク 2」へのダイヤルアップ設定。

「ダイヤルアップ接続先設定 No.3」は、「インターネット」へ接続するダイヤルアップ設定。また、「ダイヤルアップ接続先設定 No.1」と「ダイヤルアップ接続先設定 No.2」宛てのパケット以外全てのパケットは「ダイヤルアップ接続先設定 No.3」を使用するように設定。

ダイヤルアップ接続先設定 No. 1

ネットワーク 1

Tel：*99***1#

ID：user1

パスワード：user1

LAN：192.168.10.0/24

ダイヤルアップ接続先設定 No. 2

ネットワーク 2

Tel：*99***2#

ID：user2

パスワード：user2

LAN：192.168.20.0/24

ダイヤルアップ接続先設定 No. 3

インターネット

Tel：*99***3#

ID：user3

パスワード：user3

ダイヤルアップ接続先の詳細設定

No.	3
宛先IPアドレス	0.0.0.0
宛先ネットマスク	0.0.0.0
電話番号	*99***3#
ID	user3
パスワード	●●●●●
接続方式	通常ダイヤルアップ
本体側IPアドレス	0.0.0.0
メモ	インターネット

設定　キャンセル

※宛先 IP アドレス、宛先ネットマスクを 0.0.0.0 にすることで、「ネットワーク 1」／「ネットワーク 2」宛てのダイヤルアップ以外全ての宛先のダイヤルアップを行います。

設定例のダイヤルアップ接続先リスト

インターフェイス

インターフェイスの各設定を行います。

モバイル通信端末:ダイヤルアップ

ダイヤルアップ接続先リストの設定を行います。

接続先を追加する。 追加

No.	宛先IPアドレス	宛先ネットマスク	電話番号	ID	メモ	操作
1	192.168.10.0	255.255.255.0	*99***1#	user1	ネットワーク1	変更 削除
2	192.168.20.0	255.255.255.0	*99***2#	user2	ネットワーク2	変更 削除
3	0.0.0.0	0.0.0.0	*99***3#	user3	インターネット	変更 削除

戻る

4-4 接続／切断方法

1. 設定ツールのメニューから、［ステータス］－［モバイル通信端末］ をクリックします。

   「モバイル通信端末ステータス」のページが表示されます。

ステータス

現在の設定・状態を表示します。

モバイル通信端末

■ モバイル通信端末の通信状態を表示します。

No.	接続先 情報	接続先 メモ	ステータス	操作
1	*99***5# XXXXX		ダイヤルアップ接続完了 詳細表示	切断 無効

項目		内容
No.		現在接続しているダイヤルアップ接続先の設定番号を表示します。 未接続時、RAS 接続時は空白になります。
接続先 情報		現在接続しているダイヤルアップ接続先、RAS の情報（電話番号、ユーザ名）を表示します。未接続時は空白になります。
接続先 メモ		現在接続しているダイヤルアップ接続先のメモを表示します。 未接続時、RAS 接続時は空白になります。
ステータス（ダイヤルアップ接続時）		設定したダイヤルアップ接続の現在の状態が表示されます。［詳細表示］をクリックすると、現在の状態をより詳しく参照できます。 ➲ ステータスの詳細については、『モバイル通信端末のステータス一覧』をご覧ください。
操作	［接続#1～#8］	それぞれのダイヤルアップ接続先に対する接続動作を行います。
	［切断］	切断動作を行います。
	[OTASP]	利用開始登録動作を行います。 ※ RX160 のみ
	［無効］	設定を無効にします。 次回、［有効］をクリックするまで設定内容を使えないようにします。
	［有効］	設定を有効にします。 次回、［無効］になっている設定を再度使えるようにします。

モバイル通信端末のステータス一覧

ステータス表示	状態	MOBILE ランプの状態
無効	接続設定が無効になっています。	消灯
使用しない	モバイル通信端末は正常に認識されていますが、接続設定が行われていません。	消灯
未動作	モバイル通信端末が認識されていないか、SIM カードが挿入されていないか、モバイル通信端末制御サービスが一時停止しています。 モバイル通信端末の再起動を行っている時などに表示されます。	消灯
待受中	モバイル通信端末が正常に認識されていて、接続設定も行われていますが、接続が行われていない状態です。	消灯
ダイヤルアップ発信中	接続先へ電話を掛け始めた状態です。	点滅

ステータス表示	状態	MOBILE ランプの状態
ダイヤルアップ PPP ネゴ中	認証を行っている状態です。	点滅
ダイヤルアップ接続完了	接続が正常に行えた状態です。	点灯
未登録　※ RX160 のみ	利用開始登録(OTASP)していない状態です。	消灯
登録処理中 ※ RX160 のみ	利用開始登録処理中の状態です。	2 回点滅
解約処理中 ※ RX160 のみ	利用解約処理中の状態です。	2 回点滅

4-4-1　通信ステータス詳細表示

モバイル通信端末通信の詳細表示

No.	1
ステータス:	ダイヤルアップ接続完了
電話番号:	*99***1#
ユーザ名:	suncomm
IPアドレス:	
ゲートウェイ:	
DNSサーバ1:	
DNSサーバ2:	

送信バイト数:	97 バイト
送信パケット数:	5 パケット
送信エラー回数:	0 回
受信バイト数:	64 バイト
受信パケット数:	4 パケット
受信エラー回数:	0 回

戻る

項目	内容
ステータス	設定したダイヤルアップ接続の現在の状態が表示されます。
電話番号	設定したアクセスポイントへの電話番号が表示されます。
ユーザ名	設定したユーザ名が表示されます。
IP アドレス	プロバイダおよび接続先から割り当てられた、Rooster RX の WAN 側 IP アドレスが表示されます。
ゲートウェイ	ゲートウェイの IP アドレスが表示されます。
DNS サーバ 1	DNS サーバ 1 の IP アドレスが表示されます。
DNS サーバ 2	DNS サーバ 2 の IP アドレスが表示されます。
送信バイト数	モバイル通信端末で送信したデータの総バイト数が表示されます。
送信パケット数	モバイル通信端末で送信したデータの総パケット数が表示されます。
送信エラー回数	モバイル通信端末でデータ送信を行った際に発生した、エラー回数の総計が表示されます。
受信バイト数	モバイル通信端末で受信したデータの総バイト数が表示されます。
受信パケット数	モバイル通信端末で受信したデータの総パケット数が表示されます。
受信エラー回数	モバイル通信端末でデータ受信を行った際に発生した、エラー回数の総計が表示されます。

5章　着信設定

ここでは RAS 着信、WakeOn 着信の設定を行います。

5-1 RAS着信接続設定

【RAS 着信機能について】
RAS（Remote Access Service）とは、電話回線を通じて遠隔地のネットワークにダイヤルアップ接続し、そのネットワークの資源を利用する機能をいいます。

1. 設定ツールのメニューから、［インターフェイス］－［モバイル通信端末］－［RAS 着信］をクリックします。　「RAS 着信設定」のページが表示されます。

RX110　RX130

RX160　RX180

インターフェイス
インターフェイスの各設定を行います。
モバイル通信端末：RAS着信
モバイル通信端末の設定（RAS着信）を行います。
必要な場合は「ダイヤルアップ接続」および「フィルタリング」の設定を行ってください。
RAS着信接続を行う。
RAS着信モード：IP着信
本体側IPアドレス：　自動設定　IP固定
IPアドレス：
ユーザー設定：
ID：test
パスワード：
無通信監視を行う。600 秒
NATを使用する。
設定

2. ［RAS 着信接続を行う］チェックをオンにし、以下の設定を行います。

必要な場合は「ダイヤルアップ接続」および「フィルタリング」の設定を行ってください。

➲ ダイヤルアップ接続については『4-3 ダイヤルアップ接続設定』をご覧ください。

➲ フィルタリングについては『8-3　フィルタリング』をご覧ください。

RX180

➲ APN 設定の CID1 に RAS 着信を行う APN を設定してください。『4-1　APN 設定』をご覧ください。

➲ RAS 着信を使用する場合、ダイヤルアップ接続先には RAS 着信と同じ接続先以外接続できません。

<table>
<tr><th>項目</th><th>内容</th></tr>
<tr><td>RAS 着信モード</td><td>RX110 RX130
RAS 着信モードを選択します。「ビジネス mopera」のみ。

（仮想サーバ設定）※IP 着信時にアクセスする機器に設定します。
NTT ドコモのビジネス mopera アクセスプレミアムの IP 着信オプションをご利用の際には、［ビジネス mopera］を選択ください。
NTT ドコモとの契約が必要になります。
ビジネス mopera アクセスプレミアムにつきましては、NTT ドコモのホームページをご覧ください。
RX160 RX180
RAS 着信モードを選択します。「IP 着信」のみ。

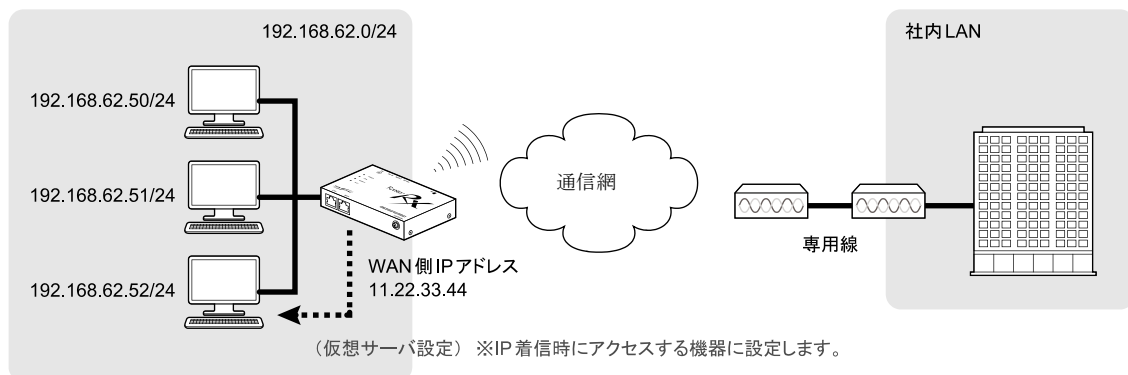
（仮想サーバ設定）※IP 着信時にアクセスする機器に設定します。
ソフトバンクまたは KDDI との契約が必要になります。</td></tr>
<tr><td>本体側 IP アドレス：自動取得</td><td>WAN 側の IP アドレスが自動取得の場合はこちらを選択します。</td></tr>
<tr><td>本体側 IP アドレス：IP 固定</td><td>本体側の IP アドレスを固定にて設定する場合に選択ください。</td></tr>
<tr><td>IP アドレス</td><td>本体側 IP アドレスを［IP 固定］で選択した際には、IP アドレスを入力します。</td></tr>
<tr><td>ユーザー設定</td><td>認証に使用する ID、パスワードを入力します。</td></tr>
<tr><td>無通信監視を行う</td><td>チェックをオンにすると、Rooster RX に指定した秒数の間、通信が行われなかった時、自動的に回線を切断するようになります。
チェックがオンになっていても、「0」を入力した場合、無通信監視は行いません。</td></tr>
<tr><td>NAT を使用する</td><td>［RAS 着信モード］で［通常］以外を選択した場合、必要に応じて設定してください。</td></tr>
</table>

3. ［設定］ボタンをクリックします。

5-1-1　ダイヤルアップ接続設定とRAS着信設定の併用

Rooster RX では、ダイヤルアップ接続設定と RAS 着信設定を併用させることが可能です。
待受中に着信があった場合は、RAS 着信の設定が有効になり、着信動作を行います。
逆に待受中に接続要求があった場合は、ダイヤルアップ接続の設定が有効となり、ダイヤルアップ動作を行います。

➲ ダイヤルアップ接続設定は、『4 章　ダイヤルアップ設定』をご覧ください。

➲ RAS 着信接続設定は、『5-1　RAS 着信接続設定』をご覧ください。

- RAS 着信接続とダイヤルアップ接続は排他接続となります。（同時にお使いいただくことはできません）
- ダイヤルアップ接続の各設定と RAS 着信接続の各設定は独立していますので、それぞれ設定してください。

5-1-2　RAS着信時のステータス表示

1. 設定ツールのメニューから［ステータス］―［モバイル通信端末］をクリックします。「モバイル通信端末ステータス」のページが表示されます。

ステータス

現在の設定・状態を表示します。

モバイル通信端末

■ モバイル通信端末での通信状態を表示します。

No.	ステータス	接続先	操作
1	着信接続完了 詳細表示	test	切断 無効

項目	内容
ステータス（RAS 着信時）	設定した RAS 着信の現在の状態が表示されます。［詳細表示］をクリックすると、現在の状態をより詳しく参照できます。 ➲ ステータスの詳細については、『モバイル通信端末のステータス一覧』をご覧ください。

モバイル通信端末のステータス一覧

ステータス表示	状態	MOBILE ランプの状態
無効	接続設定が無効になっています。	消灯
未装備	モバイル通信端末が挿入されていないか、認識できていません。	消灯
使用しない	モバイル通信端末は正常に認識されていますが、接続設定が行われていません。	消灯
待受中	モバイル通信端末が正常に認識されていて、接続設定も行われていますが、接続が行われていない状態です。	消灯
着信接続中	遠隔地からの接続機器のアクセスを確認した状態です。	点滅
着信 PPP ネゴ中	Rooster RX で、接続機器の認証を行っている状態です。	点滅
着信接続完了	着信接続が正常に行えた状態です。	点灯
未登録　※ RX160 のみ	利用開始登録(OTASP)していない状態です。	消灯
登録処理中 ※ RX160 のみ	利用開始登録処理中の状態です。	2 回点滅
解約処理中 ※ RX160 のみ	利用解約処理中の状態です。	2 回点滅

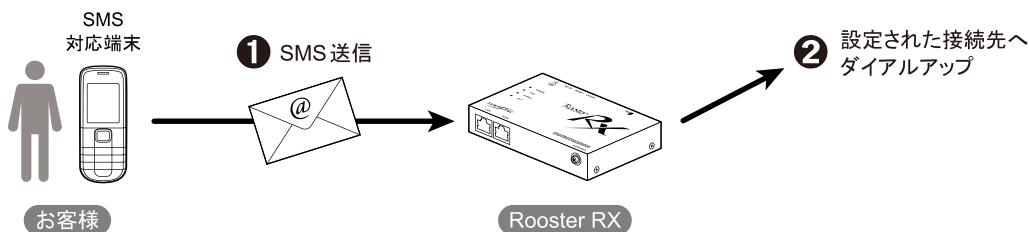
RAS 着信はモバイル通信端末ログに記録されます。

➲ ログ表示の詳細は、『9-2-1　モバイル通信端末ログ』をご覧ください。

5-2 WakeOn着信の設定

【WakeOn 着信について】
WakeOn 着信とは、待ち受け状態のモバイル通信端末を、遠隔地からの操作によりダイヤルアップさせることを可能とする機能です。
SMS による着信に対応しています。

WakeON メッセージ

memo

RX160 の場合はセンタープッシュサービス、CIPL/CRG サービスを用いた IP-PUSH によるセンターからの SMS 送信となります。

1. 設定ツールのメニューから、［インターフェイス］－［モバイル通信端末］－［WakeOn 着信］をクリックします。

   「WakeOn 着信設定」のページが表示されます。

2. ［WakeOn 着信を行う］チェックをオンにし、以下の設定を行います。

項目	内容
WakeOn 着信を行う	WakeOn 着信機能を使用する場合は、チェックをオンにします。
認証キー	WakeOn メッセージの文字列による認証を行えます。 ［WakeOn 着信を行う］設定を有効にした時に設定できます。 認証キーは、（受信したメッセージの先頭文字）～（設定された認証キー文字数）までを比較し、一致した場合は成功となります。 ただし、一文字でも異なった場合は認証失敗となります。 なお空白の場合、認証は行いません。認証キーは半角英数字のみです。 【WakeOn メッセージ認証設定例】
着番認証を行う	WakeOn を行う発信端末を限定させたい場合、チェックをオンにすると、発信者電話番号で認証を行うことができます。 オンにすると［着番リストの設定］へのリンクが有効となります。

【WakeOn メッセージ認証設定例】

設定した認証キー	受信したメッセージ	結果	
1234	5678	×	全く一致していないため
1234	1234	○	全文字一致しているため
12	1234	○	先頭 2 文字が一致しているため
12345	1234	×	5 文字目が一致しないため

認証キー文字列に、“OK” “ERROR”は使用できません。

3. ［設定］ボタンをクリックして、設定内容を反映させます。

引き続いて［着番リストの設定］も行う場合は、ここで一度、［設定］ボタンをクリックして、設定内容を反映させます。［着番リストの設定］を先にクリックすると、設定した内容が破棄されてしまいます。

5-2-1　着信番号での認証設定

1. ［着番リストの設定］をクリックします。

「WakeOn 着信相手先リスト」のページが表示されます。

2. WakeOn 着信リストの追加を行いたい場合は、［追加］ボタンをクリックします。設定済みの WakeOn 着信相手先を変更する場合は、［変更］をクリックします。
［戻る］ボタンをクリックすると、「WakeOn 着信設定画面」のページに戻ります。
［追加］ボタン、または［変更］をクリックすると、「WakeOn 着信リストの詳細設定」ページが表示されます。
［追加］ボタンをクリックした場合は空白の状態で、［変更］をクリックした場合は、設定済みの情報が入力された状態で開きます。
［削除］をクリックすると、表示されている WakeOn 着信リスト設定が削除されます。

memo　着信相手先の設定は最大 16 件まで行えます。

3. 以下の設定を行います。

項目	内容
No.	WakeOn 着信リストの通し番号が表示されます。
電話番号	WakeOn 着信相手先の電話番号を入力します。 ▶ 電話番号の－（ハイフン）は、入力してもしなくても構いません。
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶ 半角 16 文字（全角 8 文字）までの任意の文字列を入力できます。

4. ［設定］ボタンをクリックし、設定内容を反映させます。
［キャンセル］ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「WakeOn 着信相手先リスト」のページに戻ります。

- WakeOn 着信による発信は、モバイル通信端末ログに記録されます。

➲ ログ表示の詳細は、『9-2-1　モバイル通信端末ログ』をご覧ください。

5-3 緊急速報受信設定 RX130

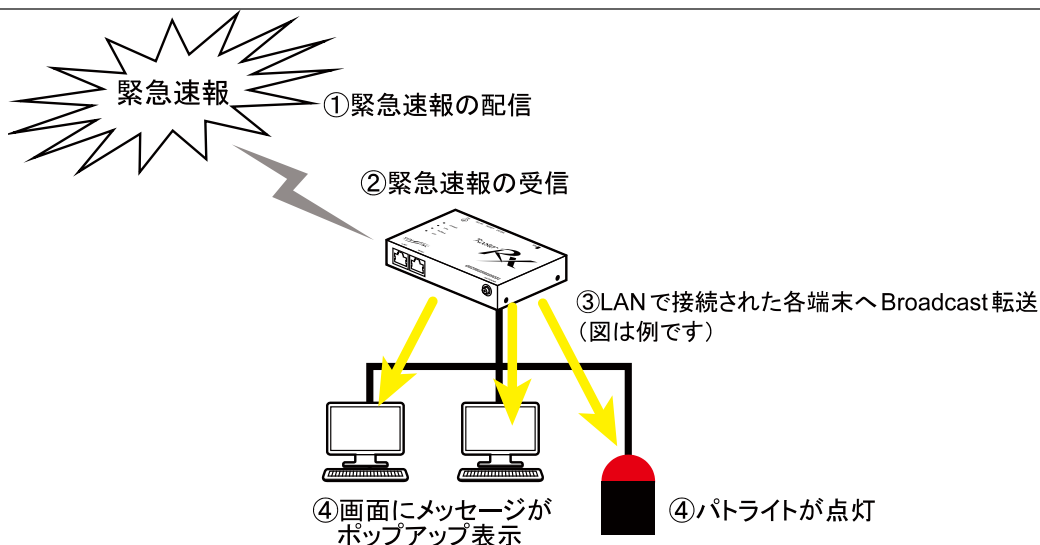
【緊急速報機能について】
緊急速報とは、気象庁が配信する緊急地震速報や津波警報、国・地方公共団体が配信する災害・避難情報を、回線混雑の影響を受けずに受信することができます。

緊急速報受信設定は、WEB 画面からは設定できません。TELNET コマンドを用いた設定のみ対応しておりますので、設定方法等は「RoosterRX TELNET 設定機能説明書」をご確認ください。
TELNET コマンドを用いて設定して頂くことで、下記の機能を実現できます。

・緊急速報の受信
・受信した緊急速報のブロードキャスト転送
・新たに受信した緊急速報の件数と、最終受信時刻の表示
・新たに受信した緊急速報の件数をクリア
・受信した緊急速報を表示
・緊急速報ブロードキャスト転送の疑似テスト

- パケット通信中およびその他の通信中、または電源を切っていたり、サービスエリア内でも電波の届かない場所（トンネル、地下など）や電波状態の悪い場所では、緊急速報を受信できない場合があります。その場合、通知を再度受信することはできませんので、ご注意ください。
- 本サービスに関して、通信障害やシステム障害による情報の不達・遅延、および情報の内容、その他当社の責に帰すべからざる事由に起因して発生したお客様の損害について、責任を負いません。
- 本サービスの詳細については、通信事業者にお問い合わせください。
- 本機能を利用される場合は、実装に必要な要件がございます。必ず、弊社サポート又は担当営業までお問い合わせください。

5-3-1 緊急速報のブロードキャスト転送

【緊急速報のブロードキャスト転送機能について】
緊急速報を RoosterRX がブロードキャスト転送することにより、お客様装置でメッセージを受信し、ポップアップを表示させたり、パトライトを点灯させたりすることができます。

本機能を使用される場合は、別途ご契約が必要となります。機密保持契約成立後、プロトコル仕様を開示させていただきます。なお、本件は法人のお客様に限らせていただきます。

6章　Rooster RXのメンテナンス

この章では、Rooster RX に設定した情報を保存したり、ファームウェアのアップデート、再起動などについて説明します。

6-1　設定情報の保存、読み込み

1. 設定ツールのメニューから、［本体設定］－［設定情報の保存、読み込み］ をクリックします。

   「設定情報の保存、読み込み」のページが表示されます。

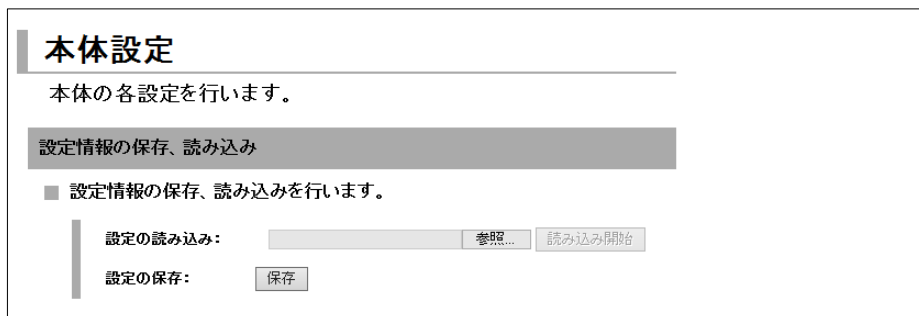
本体設定

本体の各設定を行います。

設定情報の保存、読み込み

■ 設定情報の保存、読み込みを行います。

設定の読み込み：　参照...　読み込み開始

設定の保存：　保存

6-1-1　現在の設定を保存

［現在の設定］テキストボックス内の設定情報の保存を行います。

1. ［設定の保存］の［保存］ボタンをクリックします。

   ブラウザの下部に保存確認のメッセージが表示されます。

192.168.62.1 から rooster.cfg を開くか、または保存しますか?　ファイルを開く(O)　保存(S)　キャンセル(C)

2. ［保存(S)］ボタンをクリックします。

   保存先を指定する場合は、［保存(S)］ボタン横の［▼］ボタンから［名前を付けて保存(A)］を選択して、保存先を指定します。

   Rooster RX の設定情報「rooster.cfg」が、指定した保存先にダウンロードされます。

6-1-2　保存した設定の読み込み

1. ［設定の読み込み］の［参照］ボタンをクリックし、読み込みを行う設定情報ファイル「＊.cfg」のある場所を指定します。
2. ［読み込み開始］ボタンをクリックします。

   Rooster RX の設定が保存時の設定に書き戻されます。

ファームウェアのアップデートにおいて、違ったメジャーバージョンのファームウェアの設定情報ファイルは読み込めません。

➲ 詳細につきましては『6-3　ファームウェアのアップデート方法』をご覧ください。

6-2 設定情報の消去

1. 設定ツールのメニューから、［本体設定］ー［設定の消去］ をクリックします。

   「設定の消去」のページが表示されます。

   本体設定

   本体の各設定を行います。

   設定の消去

   ■ 設定情報を消去して出荷時の状態に戻します。

   工場出荷時の設定に戻す　消去

2. ［工場出荷時の設定に戻す］の 消去 ボタンをクリックします。

   確認ダイアログで［OK］をクリックすると、Rooster RX が再起動し、設定が工場出荷時の状態にリセットされます。

設定情報の初期化は、Rooster RX 本体にある RESET スイッチの長押しでも行うことができます。

➔ 詳細は『1-5　各部の名称と機能』の RESET スイッチの項目をご覧ください。

6-3 ファームウェアのアップデート方法

ファームウェアのアップデートにおいて、違うメジャーバージョンへアップデートする場合、設定情報がすべて工場出荷時に初期化されます。
WEB 設定画面における「設定情報の保存・読み込み」もできませんのでご了承ください。

【ファームウェアのバージョン情報の見方】

マイナーバージョン番号

RRX1X0-1.2.0, Feb 10 2014 22:00:18

機種番号　メジャーバージョン番号

現状のファームウェアのバージョンをご確認いただき、アップデートするファームウェアのメジャーバージョンが違う場合は、設定情報が引き継げません。（工場出荷時に初期化されます）
マイナーバージョン番号のみの場合は、設定情報は引き継がれます。

1. 設定ツールのメニューから、[本体設定]－[ファームウェアアップデート]をクリックします。「ファームウェアのアップデート」ページが表示されます。

例）RX110 の場合(その他の機種は、機種番号がそれぞれ異なります。)

本体設定

本体の各設定を行います。

ファームウェアアップデート

■ ファームウェアのアップデートを行います。

現在のファームウェアバージョン:

RRX110-1.2.0, Feb 10 2014 22:00:18

アップデート開始ボタンを押すと、指定されたファームウェアに書き換えを行います。

ファイル名: [参照...] [アップデート開始]

2. ［参照］ボタンをクリックして、ダウンロードしたアップデートプログラムデータ「＊.img」のある場所を指定します。

3. ［アップデート開始］ボタンをクリックします。

確認ダイアログで［OK］をクリックすると、Rooster RX のファームウェアがアップデートされます。

- アップデートを実行すると、SNMP 機能を使用している場合強制停止されます。

➔ SNMP 機能の詳細につきましては、『7-6　SNMP サービス』をご覧ください。

- ファームウェアのマイナーバージョンアップデートは、メジャーバージョン番号が一致している必要があります。また、マイナーバージョンのアップデートは、新しいバージョンへのアップデートのみ可能です。（古いバージョンへ戻すことができません）
- ファームウェアのイメージファイルは 10M バイト以上あります。従量課金のご契約でのダウンロードにはご注意ください。

!! ファームウェアのアップデートでは完了するまで、10 分程度かかります。アップデート中は、絶対に電源が OFF とならないようにしてください。動作不能となる恐れがあります。これにより動作不能となった場合、有償修理となりますのでご注意願います。

6-4 再起動

1. 設定ツールのメニューから、［本体設定］－［再起動］をクリックします。

「再起動」ページが表示されます。

本体設定

本体の各設定を行います。

再起動

本体を再起動させます。

再起動ボタンを押すと、本体が再起動します。 再起動

2. ［再起動］ボタンをクリックします。

! 再起動が完了するまで、1 分程度かかります。

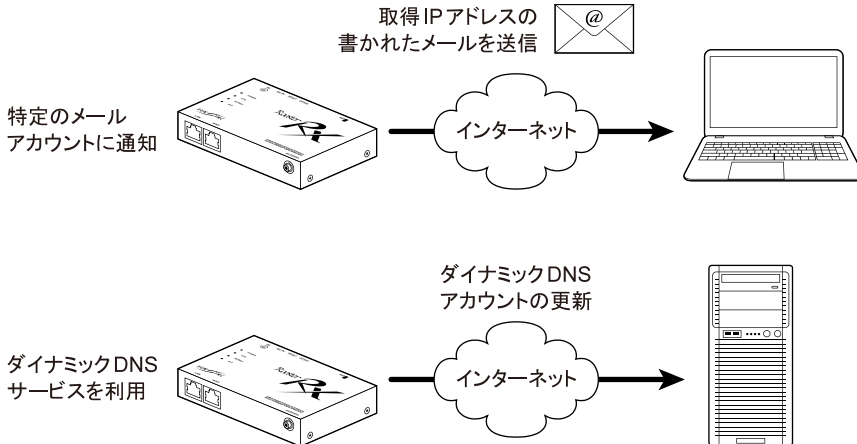
6-5 モバイル通信端末のメンテナンス

! モバイル通信端末の情報表示や制御を TELNET コマンドで行うことができます。
・PIN1 コードの設定/解除
・モバイル通信端末の自動リセット設定、自動リセット時間間隔設定
・電話番号、IMEI、アンテナレベル、その他モバイル通信端末情報の表示
・モバイル通信端末のリセット
詳しくは「TELNET 設定機能説明書」をご覧ください。

7章　各種サービス設定

この章では、ネットワークをより快適に利用するための各種サービスの設定について説明します。

7-1 アドレス解決機能

【アドレス解決機能について】
外部ネットワークから、インターネットに接続された Rooster RX にアクセスする場合、Rooster RX に割り当てられたグローバル IP アドレスの情報が必要になりますが、通常のインターネット接続ではインターネットに接続するたびに、グローバル IP アドレスは任意に変化します。
Rooster RX では、変化するグローバル IP アドレスを指定メールアカウントに通知する機能、ダイナミック DNS サーバを利用する機能のいずれかの方法によって、上記問題を解決することができます。

1. 設定ツールのメニューから、［各種サービス］－［アドレス解決］をクリックします。
   「アドレス解決設定」のページが表示されます。

各種サービス

各種サービスの設定を行います。

アドレス解決

アドレス解決の設定を行います。

☑ アドレス解決機能を使用する。

更新時間の間隔： 0 分 （0の場合、自動更新）

○ 特定のメールアカウントに通知する。

メールアカウントの設定

送信先メールアドレス：

送信元メールアドレス：

メール送信の設定：

◉ 標準のメッセージを送信する。 ○ 指定のメッセージを送信する。

指定のメッセージ：

（IPアドレスは、'%s'と表記してください。）

◉ ダイナミックDNSサービスを利用する。

サービスの種類： suncomm.DDNS

サーバ名： www.suncomm.jp

ホスト名： suncomm.suncomm.net

アカウント： suncomm

パスワード： •••••••

設定

アドレス解決機能を使用する場合は、［アドレス解決機能を使用する］チェックをオンにし、以下の設定を行います。

7-1-1　IPアドレスを指定メールアカウントに通知する設定

1. ［特定のメールアカウントに通知する］チェックをオンにし、以下の設定を行います。

項目	内容
更新時間の間隔	指定メールアカウントに、設定された時間ごとにメール送信します。「0」を設定した場合自動更新となり、グローバル IP アドレスが変更された時のみ、メール送信を行います。 「0」以外を設定される場合、設定の最小値は 5（分）となります。
メールアカウントの設定	➲ 設定方法は『3-5　メールアカウントの設定』をご覧ください。 ❗ 引き続いて［メールアカウントの設定］も行う場合は、ここで一度［設定］ボタンをクリックして、設定内容を反映させます。［設定］ボタンより先に［メールアカウント設定］をクリックすると、設定した内容が破棄されます。
送信先メールアドレス	グローバル IP アドレスを通知させたいメールアドレスを入力します。 ▶ 送信先メールアドレスを複数先設定したい場合は、「,（カンマ）」区切りで設定いただけます。設定可能文字数は区切りの「,（カンマ）」を含めて 63 文字までです。
送信元メールアドレス	送信者のメールアドレスを入力します。 ❗ 送信元メールアドレスの入力がないと、メールサーバによってはメールが送信されない場合があります。
メール送信の設定	通知メールのメッセージ内容を指定したい場合は、［指定のメッセージを送信する］を選択します。必要がなければ、［標準のメッセージを送信する］を選択します。 標準のメッセージは、以下のような形式で送信されます。 【送信メールの例】 タイトル：Rooster IP Report 送信者：Rooster（004053010203）⇒ カッコ内は Rooster RX の MAC アドレス 内容：Rooster IP-Address Report v0.01. MAC=004053010203 ⇒ Rooster RX の MAC アドレス IP=10.20.30.40 ⇒ 割り当てられるグローバル IP アドレス 文字列を指定して入力を行う場合、指定のメッセージ入力フォームに、「%s」（「 」は不要）と入力すると、取得したグローバル IP アドレスに変換されて通知されます。 ▶【割り当てグローバル IP アドレスが”11.22.33.44”の場合】 設定内容：http://%s/mobile 実際に送信されるメッセージ：http://11.22.33.44/mobile

2. ［設定］ボタンをクリックして、設定内容を反映させます。

7-1-2　ダイナミックDNSサービスを利用する設定

1. ［ダイナミック DNS サービスを利用する］チェックをオンにし、以下の設定を行います。

項目	内容
更新時間の間隔	指定されたダイナミック DNS サービスへ、設定された時間ごとに更新を行います。「0」を設定した場合自動更新となり、グローバル IP アドレスが変更された時のみ、ダイナミック DNS サービスへの更新を行います。 「0」以外を設定される場合、設定の最小値は 5（分）となります。
サービスの種類	アドレス解決に使用するダイナミック DNS サービスを選択します。 「suncomm.DDNS」のみの設定です。 ダイナミック DNS サービスを使用される場合は、別途契約または登録が必要となります。詳細につきましては、下記の URL をご覧ください。 「suncomm.DDNS」 http://www.sun-denshi.co.jp/sc/ddns/index.html ▶ サン電子（株）が運用する有償でのダイナミック DNS サービスです。別途、ご契約が必要となりますので、上記 URL をご覧ください。また、「suncomm.DDNS」機能を利用して、お客様独自にダイナミック DNS サーバを設置・運用いただくことも可能です。「suncomm.DDNS」のプロトコル仕様につきましては、機密保持契約成立後、開示させていただきます。なお、本件は法人のお客様に限らせていただきます。

2. ［サーバ名］、［ホスト名］、［アカウント］、［パスワード］を入力します。
3. ［設定］ボタンをクリックして、設定内容を反映させます。

7-2 DNSサービス

1. 設定ツールのメニューから、［各種サービス］－［DNS サービス］をクリックします。
   「DNS サービス設定」のページが表示されます。

2. DNS リレー機能を使用する場合、［DNS リレー機能を使用する］チェックをオンにします。
3. ［設定］ボタンをクリックして、設定内容を反映させます。

DNS リレー機能を使用するかしないかによって、接続機器 TCP/IP 設定の DNS サーバ設定方法が異なってきます。以下のうち該当する設定を行ってください。

DNSリレー機能を使用する場合。

下記のいずれかの設定を行います。

- DNS サーバアドレスを自動的に取得するように設定します。
- DNS サーバアドレスを指定する場合、Rooster RX の LAN IP アドレス、またはプロバイダ指定の DNS サーバ（ネームサーバ）アドレスを指定します。

DNSリレー機能を使用しない設定の場合。

自動取得されないので、指定する必要があります。
プロバイダ指定の DNS サーバ（ネームサーバ）アドレスを指定します。

7-3 DHCPサービス

1. 設定ツールのメニューから、［各種サービス］－［DHCP サービス］をクリックします。
   「DHCP サービス設定」のページが表示されます。

2. DHCP 機能を使用する場合、［DHCP 機能を使用する］チェックをオンにします。
3. DHCP 機能の［方式］として［DHCP サーバ］を選択します。
   【DHCP サーバの場合】
   Rooster RX 自身を DHCP サーバとして動作させたい場合に設定します。

項目	内容
リース開始 IP アドレス	割り当てる IP アドレスの開始アドレスを入力します。
個数	DHCP サーバ機能で使用する、リース開始 IP アドレスからのアドレスの個数を指定します。 ▶初期設定では、［リース開始 IP アドレス］が「192.168.62.50」、［個数］が「50」と設定されているので、「192.168.62.50～192.168.62.99」が、DHCP サーバ機能で使用する IP アドレスの範囲となります。
プライマリ DNS サーバ	DHCP で配布する DNS サーバを指定します。
セカンダリ DNS サーバ	DHCP で配布する DNS サーバを指定します。

この他に、DHCP のリースタイムの設定ができる TELNET コマンドがあります。詳しくは「TELNET 設定機能説明書」をご覧ください。

4. ［設定］ボタンをクリックして、設定内容を反映させます。

Rooster RX の DHCP テーブルは、設定ツールのメニューから、［ステータス］－［DHCP 割り当て一覧］をクリックして表示される「DHCP 割り当て表示画面」から確認することができます。

項目	内容
IP アドレス	Rooster RX LAN 内にある LAN 接続機器に割り当てた IP アドレスが表示されます。
MAC アドレス	上記の IP アドレスを付与された、LAN 接続機器の MAC アドレスが表示されます。 ❗ Rooster RX を再起動すると、DHCP テーブルはすべてリセットされます。 ❗ 再起動後、クライアントからの IP アドレス割り当て要求を受けたタイミングで、再度 DHCP テーブルに登録されます。

7-4 TELNETサービス

TELNET サービスによって、Web 設定ツールで設定可能なすべての項目を設定できます。
▶設定ツールで行えない設定も一部可能です。

➲ TELNET コマンドの詳細は、『TELNET 設定機能説明書』をご覧ください。

1. 設定ツールのメニューから、［各種サービス］－［TELNET サービス］をクリックします。「TELNET サービス設定」のページが表示されます。

2. TELNET サービスを使用する場合、［TELNET サービスを使用する］チェックをオンにします。
3. ［ポート番号］で、TELNET サービスで使用するポート番号を入力します。
4. 以下の設定を行います。

項目	内容
LAN ポートからのアクセスを許可する	チェックをオンにすると、LAN ポートからの TELNET ログインができます。 オフにすると、LAN ポートからの TELNET ログインを拒否します。
外部からのアクセス	WAN 側からの TELNET ログイン（設定ツールへのログイン）を許可するポリシーを設定します。 ［許可しない］、［全て許可する］、［INPUT フィルタリングに従う］から選択します。

5. ［設定］ボタンをクリックして、設定内容を反映させます。

7-5 Webサービス

【Web サービスについて】
Web サービスは、Rooster RX の設定ツールにアクセスを行う機能です。
設定により LAN ポートまたは WAN から、設定ツールにアクセスできるポートを決定することができます。

1. 設定ツールのメニューから、［各種サービス］－［Web サービス］をクリックします。
「Web サービス設定」のページが表示されます。

2. Web サービスを使用する場合、［Web サービスを使用する］チェックをオンにします。
3. ［ポート番号］で、Web サービスで使用するポート番号を入力します。
4. 以下の設定を行います。

項目	内容
LAN ポートからのアクセスを許可する	チェックをオンにすると、LAN ポートからの設定ツールへのログインができます。 オフにすると、LAN ポートからのログインができません。
外部からのアクセスを許可する	WAN 側からの設定ツールへのログインを許可するポリシーを設定します。 ［許可しない］、［全て許可する］、［INPUT フィルタリングに従う］から選択します。

5. ［設定］ボタンをクリックして、設定内容を反映させます。

7-6 SNMPサービス

【SNMP について】
SNMP（Simple Network Management Protocol）は、ネットワーク機器の状態をネットワーク経由で問い合わせたり、それに答えたりするための通信手順の一つをいいます。
SNMP を使用することによって、ネットワーク管理を容易に行うことができるようになります。
SNMP コミュニティは、監視する側のネットワーク監視端末（SNMP マネージャ）と、監視される側のネットワーク上の機器（SNMP エージェント）により構成され、このうち Rooster RX は、SNMP エージェントとしての動作に対応しております。
対応バージョンは、SNMPv1 のみとなります。

1. 設定ツールのメニューから、［各種サービス］－［SNMP］をクリックします。
「SNMP 設定」のページが表示されます。

各種サービス
各種サービスの設定を行います。
SNMPサービス
■ SNMPサービスの設定を行います。
☑ SNMPサービスを使用する。
SNMPマネージャIPアドレス： 192.168.62.50
（未設定時は、すべてのIPアドレスからのアクセスを許可する。）
コミュニティ名： suncomm
SYSLocation名：
☑ SNMP TRAPを使用する。
☑ LANポートからのアクセスを許可する。
☐ 外部からのアクセスを許可する。
設定

2. SNMP 機能を使用する場合、「SNMP 機能を使用する」チェックをオンにします。
3. 以下の設定を行います。

項目	内容
SNMP マネージャ IP アドレス	SNMP マネージャのローカル IP アドレスを設定します。
コミュニティ名	SNMP マネージャと Rooster RX がやり取りを行うためのコミュニティ名を設定します。最大 16 文字まで設定できます。
SYSLocation 名	MIB 変数の SYSLocation 名を設定します。
SNMP TRAP を使用する	Rooster RX から、SNMP マネージャ IP アドレス宛に SNMP TRAP を送信する場合、チェックをオンにします。
LAN ポートからのアクセスを許可する	チェックをオンにすると、LAN ポートからのアクセスができます。 オフにすると、LAN ポートからのアクセスができません。
外部からのアクセスを許可する	チェックをオンにすると、WAN 側からのアクセスができます。 オフにすると、WAN 側からのアクセスができません。

4. ［設定］ボタンをクリックして、設定内容を反映させます。

7-7 WANハートビート機能

【WAN ハートビート機能について】
WAN ハートビート機能は、WAN 側のネットワークが正常に動いているかどうかの確認を行うための機能です。

1. 設定ツールのメニューから、［各種サービス］－［WAN ハートビート］をクリックします。
「WAN ハートビート設定」のページが表示されます。

各種サービス
各種サービスの設定を行います。
WANハートビート
WANハートビートの設定を行います。
WANハートビートを使用する。
監視時間: 1 分
無応答時の動作: 無応答が連続して発生した場合、本機をリセットする。
WANハートビートログを記録する。
監視先IPアドレスの指定
WANのゲートウェイ
手動設定する IPアドレス: 192.168.1.1 VPN接続先
設定

2. WAN ハートビートを使用する場合、［WAN ハートビートを使用する］チェックをオンにします。
3. 以下の設定を行います。

項目	内容
監視時間	設定された間隔で WAN ハートビートを実行します。「0」を設定した場合、Rooster RX 再起動直後のみ WAN ハートビートを実行します。「0」以外を設定される場合、設定の最小値は 1（分）となります。
無応答時の動作	WAN ハートビートで、接続状態の確認ができなかった場合に行う動作を選択します。 • 無応答が連続して発生した場合、本機をリセットする。10 回（工場出荷時状態）連続して失敗した時点で、Rooster RX を再起動します。 • WAN ハートビートログを記録する。再起動は行わず、設定された監視時間ごとに WAN ハートビートログに「失敗」のログを記録します。
監視先 IP アドレスの指定	WAN ハートビートを行う相手先を指定します。相手先 IP アドレスまたは、ドメイン名を手動で設定することもできます。 指定する IP アドレスはグローバル IP アドレスまたは VPN 接続先のネットワーク IP アドレスです。 VPN 接続先のネットワーク IP アドレスに指定した場合は、VPN 接続先のチェックをオンにしてください。

この他に、WAN ハートビートのタイムアウト回数の設定ができる TELNET コマンドがあります。詳しくは「TELNET 設定機能説明書」をご覧ください。

4. ［設定］ボタンをクリックして、設定内容を反映させます。

- 従量制課金でご契約の場合は、設定しないようにしてください。意図しない接続で通信料金が掛かってしまう原因となりますので、くれぐれもご注意願います。
- WAN 側のゲートウェイ機器の仕様により、WAN ハートビートによる ping に応答しない場合があります。ping に応答しない場合は手動設定にて IP アドレスを入力するか、［WAN ハートビートログを記録する］を選択ください。
- WAN ハートビート機能は、以下の理由により無通信監視時間の設定と併用できません。
  【（無通信監視時間）＜（WAN ハートビート監視時間）の場合】
  無通信監視時間で一旦切断されても、WAN ハートビートで再度、自動発信を行ってしまいます。
  【（無通信監視時間）＞（WAN ハートビート監視時間）の場合】
  無通信監視時間で切断される前に、WAN ハートビートの通信により無通信状態がリセットされてしまい切断されません。

➔ 無通信監視時間の設定については『4-3　ダイヤルアップ接続設定』をご覧ください。

7-8 ログ管理

1. 設定ツールのメニューから、［各種サービス］－［ログ管理］をクリックします。

   「ログ管理設定」のページが表示されます。

2. ［パケット通信ログを記録する］チェックをオンにすると、［ログ］－［パケット通信ログ］の［通過ログ］、［遮断ログ］が有効になります。

   ➲ パケット通信ログの詳細は、『9-1　パケット通信ログ』をご覧ください。

3. Syslog サーバでログ管理を行いたい場合、［Syslog サーバに送信する］チェックをオンにし、Syslog サーバのローカル IP アドレスを入力します。この設定を行った場合、Rooster RX で取得できるすべてのログを Syslog サーバへ送信します。
4. ［PPP ログを記録する］チェックをオンにすると［ログ］－［サービスログ］の［PPP ログ］が有効になります。

   ➲ PPP ログの詳細は、『9-3-4　PPP ログ』をご覧ください。

5. ［設定］ボタンをクリックして、設定内容を反映させます。

7-9 位置測位機能 RX160

- 位置測位情報の取得は、WEB 画面からはできません。TELNET コマンドのみ対応しておりますので、操作方法は「RoosterRX TELNET 設定機能説明書」をご確認ください。
- TELNET コマンド入力後、位置情報を取得するまでに時間が掛かる場合があります。その場合、TELNET コマンドはタイムアウトしますので、再度コマンドを入力してください。
- 位置測位情報の取得にはパケット通信を伴いますので、『4-3　ダイヤルアップ接続設定』が必要になります。
- 位置測位情報の取得にはダイヤルアップ接続先リストの最後に登録されている接続先を使用します。
- 回線接続中に位置測位情報の取得を行う場合は、回線接続に使用した接続先以外のダイヤルアップ接続先の登録が必要になります。また、回線接続に使用したドメインと同一のものは使用できません。
- 回線待受中に位置測位情報の取得を行うだけの場合は、ダイヤルアップ接続先の登録は 1 つで使用できます。

ダイヤルアップ接続先の設定例（回線接続中に位置測位情報の取得を行う場合）

(1) 『4-3-1　ダイヤルアップ接続先の追加、変更方法』を参考に回線接続に使用するダイヤルアップ設定を行う。

(2) 『4-3-1　ダイヤルアップ接続先の追加、変更方法』を参考に位置測位で使用するダイヤルアップ設定を行う。

(3)下記のように２つのリストが作成された場合、「No.2」の接続先が位置測位で使用される。

インターフェイス

インターフェイスの各設定を行います。

モバイル通信端末:ダイヤルアップ

■ ダイヤルアップ接続先リストの設定を行います。

接続先を追加する。 追加

No.	宛先IPアドレス	宛先ネットマスク	電話番号	ID	メモ	操作
1			*99	user@au.au-net.ne.jp	回線接続用	変更 削除
2			*99	locate@locate	位置測位用	変更 削除

戻る

※設定例の設定値は例ですので、ご契約のインターネットサービスプロバイダ（以下プロバイダ）等からご提供された情報を正しくご入力ください。

TELNET コマンド入力後、位置情報が取得できた場合は下記のように表示されます。

LOCATE：＜緯度＞,＜経度＞,＜標高＞
＜緯度＞ -90.00000 ～ +90.00000 degree 設定時の緯度。小数点以下 5 桁まで表示。 北緯(+)南緯(-) (ex. +35.36000) ＜経度＞ -180.00000 ～ +180.00000 degree 設定時の経度。小数点以下 5 桁まで表示。 東経(+)西経(-) (ex. +138.72800) ＜標高＞ -999～9999 海抜高度。メートル単位。 取得不可時はブランク。
例）北緯 35.70000 度、東経 139.77616 度、標高 17m の場合 LOCATE：+35.70000,+139.77616,17

- 本機能は、測位の過程で GPS 測位サーバとパケット通信を行いますので、通信費用にご注意ください。
- 本機能は、位置情報の目安としてご利用ください。

8章　ネットワーク設定

この章では、VPN やフィルタリングなど、詳細なネットワーク設定について説明します。

8-1 VPNパススルー

【VPN パススルーについて】
VPN パススルーの設定を行うと、Rooster RX 以外の別の端末が VPN サーバやクライアントとして動作する時、各 VPN プロトコルを通過させることができるようになります。
VPN パススルーは 1 セッションのみとなります。

1. 設定ツールのメニューから、［ネットワーク］ー［パススルー］をクリックします。
「VPN パススルー設定」のページが表示されます。

2. 通過させる VPN プロトコルのチェックをオンにします。
3. ［設定］ボタンをクリックして、設定内容を反映させます。

8-2 スタティックルーティング

1. 設定ツールのメニューから、［ネットワーク］－［スタティックルーティング］をクリックします。

   「スタティックルーティング」リストのページが表示されます。

ID	ネットワーク	サブネットマスク	ゲートウェイ	インターフェイス	メモ	操作
1	11.22.33.44	255.255.255.0	55.66.77.88	LAN	static	変更 削除

2. スタティックルートの追加を行いたい場合は、［追加］ボタンをクリックします。設定済みのスタティックルーティング設定を変更する場合は、［変更］をクリックします。［削除］をクリックすると、表示されている設定が削除されます。

   ［追加］ボタン、または［変更］をクリックすると、「スタティックルーティングの詳細設定」ページが表示されます。［追加］ボタンをクリックした場合は空白の状態で、［変更］をクリックした場合は、設定済みの情報が入力された状態で開きます。

memo スタティックルートの設定は最大 128 件まで行えます。

スタティックルーティングの詳細設定

No.	1
ネットワーク	11.22.33.44
サブネットマスク	255.255.255.0
ゲートウェイ	55.66.77.88
インターフェイス	LAN
メモ	static

設定　キャンセル

3. 以下の設定を行います。

項目	内容
ネットワーク	宛先ネットワークアドレスを入力します。
サブネットマスク	上記ネットワークのサブネットマスクを入力します。
ゲートウェイ	上記ネットワークのゲートウェイアドレスを入力します。
インターフェイス	この設定を適用するインターフェイスを選択します。［WAN］、［PPPoE］、［モバイル通信端末］、［IPsec］、［LAN］のいずれかを選択します。
メモ	設定内容を分かりやすくするための覚え書きを入力します。▶半角 16 文字（全角 8 文字）までの任意の文字列を入力できます。

4. ［設定］ボタンをクリックすると、「スタティックルーティング」リストのページに戻り、設定した内容が反映されます。［キャンセル］ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「スタティックルーティング」のリストのページに戻ります。

8-3 フィルタリング

8-3-1 FORWARDフィルタリング

1. 設定ツールのメニューから、［ネットワーク］－［フィルタリング］－［FORWARD］をクリックします。

「FORWARD フィルタリング」リストのページが表示されます。

ネットワーク

ネットワークの各設定を行います。

FORWARDフィルタリング

■ FORWARDフィルタリングの設定を行います。

基本ポリシー 設定されていないパケットはすべて遮断する。 設定

設定の追加 追加

工場出荷時状態に戻す 初期化

No.	インターフェイス	方向	動作	プロトコル	相手IPアドレス	相手ポート	メモ	操作
1	全て	送信	許可	TCP		80 - 80	HTTP	変更 削除
2	全て	送信	許可	UDP		53 - 53	DNS	変更 削除
3	全て	送信	許可	TCP		25 - 25	SMTP	変更 削除
4	全て	送信	許可	TCP		110 - 110	POP3	変更 削除
5	全て	送信	許可	TCP		1720 - 1720	NetMeeting	変更 削除
6	全て	送信	許可	TCP		1503 - 1503	NetMeeting	変更 削除
7	全て	送信	許可	TCP		443 - 443	SSL	変更 削除
8	全て	送信	許可	ICMP		-	ICMP	変更 削除
9	全て	送信	許可	TCP		21 - 21	FTP	変更 削除
10	全て	送信	許可	UDP		123 - 123	NTP	変更 削除
11	全て	送信	許可	TCP		23 - 23	TELNET	変更 削除
12	全て	受信	許可	TCP		23 - 23	TELNET	変更 削除
13	全て	受信	許可	TCP		80 - 80	HTTP	変更 削除
14	全て	受信	許可	TCP		21 - 21	FTP	変更 削除
15	全て	受信	許可	ICMP		-	ICMP	変更 削除
16	全て	送信	許可	TCP		587 - 587	OP25B	変更 削除

2. FORWARD フィルタリング設定を行った項目以外のパケットをどう処理するかにより、「基本ポリシー」の
   - 「設定されていないパケットはすべて通す」
   - 「設定されていないパケットはすべて遮断する」

   のうちいずれかを選択します。

- 設定済みの項目につきましては、「基本ポリシー」の設定に関わらず、個別に設定した動作が適用されます。
- IPsec 間の通信は、この設定に関わらず、基本ポリシーは「すべて通す」設定で固定となります。

➔ IPsec 設定の詳細は、『8-6　IPsec』をご覧ください。

3. FORWARD フィルタリング設定の追加を行いたい場合は、［追加］ボタンをクリックします。設定済みの FORWARD フィルタリング設定を変更する場合は、［変更］をクリックします。［削除］をクリックすると、表示されている設定が削除されます。
   ［追加］ボタン、または［変更］をクリックすると、「FORWARD フィルタリングの詳細設定」ページが表示されます。［追加］ボタンをクリックした場合は空白の状態で、［変更］をクリックした場合は、設定済みの情報が入力された状態で開きます。

memo
FORWARD フィルタリングの設定は最大 128 件まで行えます。

FORWARDフィルタリングの詳細設定

No.	17
インターフェイス	全て
方向	受信
動作	許可
プロトコル	TCP
プロトコル番号	
相手IPアドレス	11.22.33.44
相手ポート	8080 – 8080
メモ	WEB

設定　キャンセル

4. 以下の設定を行います。

項目	内容
No.	FORWARD フィルタリング設定の通し番号が表示されます。
インターフェイス	この設定を適用するインターフェイスを選択します。 ［モバイル通信端末］、［WAN］、［PPPoE］、［全て］のいずれかを指定します。
方向	［受信］、［送信］のいずれかを指定します。
動作	［許可］、［遮断］のいずれかを指定します。
プロトコル	［全て］、［UDP］、［TCP］、［ICMP］、［ユーザ指定］のいずれかを指定します。 ［ユーザ指定］の場合は、プロトコル番号も指定します。
プロトコル番号	［プロトコル］にて「ユーザ指定」を選択した場合は、プロトコル番号を設定します。
相手 IP アドレス	FORWARD フィルタリングを行う宛先 IP アドレスを設定します。
相手ポート	FORWARD フィルタリングを行うポート番号を、1〜65535 の番号で範囲指定します。
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶半角 16 文字（全角 8 文字）までの任意の文字列を入力できます。

5. ［設定］ボタンをクリックすると、「FORWARD フィルタリング」リストのページに戻り、設定した内容が反映されます。［キャンセル］ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「FORWARD フィルタリング」のリストのページに戻ります。

memo

FORWARD フィルタリング設定を工場出荷時の状態に戻す場合は、［初期化］ボタンを押すか、下記の表をご覧いただき、フィルタリングの再設定を行ってください。

工場出荷時の FORWARD フィルタリングの設定

No.	I/F	方向	動作	プロトコル	相手 IP アドレス	相手 ポート	メモ
1	全て	送信	許可	TCP		80-80	HTTP
2	全て	送信	許可	UDP		53-53	DNS
3	全て	送信	許可	TCP		25-25	SMTP
4	全て	送信	許可	TCP		110-110	POP3
5	全て	送信	許可	TCP		1720-1720	NetMeeting
6	全て	送信	許可	TCP		1503-1503	NetMeeting
7	全て	送信	許可	TCP		443-443	SSL
8	全て	送信	許可	ICMP		ー	ICMP
9	全て	送信	許可	TCP		21-21	FTP
10	全て	送信	許可	UDP		123-123	NTP
11	全て	送信	許可	TCP		23-23	TELNET
12	全て	受信	許可	TCP		23-23	TELNET
13	全て	受信	許可	TCP		80-80	HTTP
14	全て	受信	許可	TCP		21-21	FTP
15	全て	受信	許可	ICMP		ー	ICMP
16	全て	送信	許可	TCP		587-587	OP25B

memo

工場出荷時では、『工場出荷時の FORWARD フィルタリングの設定』以外はすべて遮断されます。
それ以外のプロトコルを通過させたい場合は、新たにフィルタリングの設定を行う必要があります。

8-3-2　INPUTフィルタリング

1. 設定ツールのメニューから［ネットワーク］ー［フィルタリング］ー［INPUT］をクリックします。
   「INPUT フィルタリング」リストのページが表示されます。

2. INPUT フィルタリングの追加を行う場合は、［追加］ボタンをクリックします。既存の設定を変更する場合は、［変更］をクリックします。
   ［削除］をクリックすると、表示されている設定が削除されます。
   ［追加］ボタン、または［変更］をクリックすると、「INPUT フィルタリングの詳細設定」ページが表示されます。［追加］ボタンをクリックした場合は空白の状態で、［変更］をクリックした場合は、設定済みの情報が入力された状態で開きます。

memo
INPUT フィルタリングの設定は最大 64 件まで行えます。

INPUTフィルタリングの詳細設定

No.	1
動作	許可
プロトコル	TCP
相手IPアドレス	11.22.33.44
ネットマスク	255.255.255.254
相手ポート	8080 – 8080
メモ	WEB

設定　キャンセル

3. 以下の設定を行います。

項目	内容
No.	INPUT フィルタリング設定の通し番号が表示されます。
動作	INPUT フィルタリングの動作を指定します。［許可］のみ。
プロトコル	［UDP］、［TCP］のいずれかを指定します。
相手 IP アドレス	INPUT フィルタリングを行う相手 IP アドレスを設定します。
ネットマスク	INPUT フィルタリングを行う相手サブネットマスクを指定します。
相手ポート	INPUT フィルタリングを行うポート番号を、1〜65535 の番号で範囲指定します。
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶半角 16 文字（全角 8 文字）までの任意の文字列を入力できます。

4. ［設定］ボタンをクリックすると、「INPUT フィルタリング」リストのページに戻り、設定した内容が反映されます。［キャンセル］ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「INPUT フィルタリング」のリストのページに戻ります。

8-3-3　MACフィルタリング

【MAC フィルタリング機能について】
MAC フィルタリング機能は、LAN 側から指定した MAC アドレスの受信パケットを WAN 側ネットワークへ送信するかどうかを制御する機能です。

1. 設定ツールのメニューから、［ネットワーク］－［フィルタリング］－［MAC アドレス］をクリックします。

   「MAC フィルタリング」リストのページが表示されます。

2. MAC フィルタリングを使用する場合、［MAC フィルタリングを使用する］チェックをオンにします。

［MAC フィルタリングを使用する］チェックを ON にすると、MAC フィルタリング設定で指定した機器以外、WAN 側ネットワークへ通信できなくなります。必ず MAC アドレスを設定してください。

3. MAC フィルタリング設定の追加を行いたい場合は、［追加］ボタンをクリックします。設定済みの MAC フィルタリング設定を変更する場合は、［変更］をクリックします。［削除］をクリックすると、表示されている設定が削除されます。
［追加］ボタン、または［変更］をクリックすると、「MAC フィルタリングの詳細設定」ページが表示されます。
［追加］ボタンをクリックした場合は空白の状態で、［変更］をクリックした場合は、設定済みの情報が入力された状態で開きます。

memo MAC フィルタリングの設定は最大 32 件まで行えます。

4. 以下の設定を行います。

項目	内容
No.	MAC フィルタリング設定の通し番号が表示されます。
MAC アドレス	WAN 側ネットワークへの送信を許可したい MAC アドレスを設定します。(XX:XX:XX:XX:XX:XX)
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶ 半角 16 文字（全角 8 文字）までの任意の文字列を入力できます。

5. ［設定］ボタンをクリックすると、「MAC フィルタリング」リストのページに戻り、設定した内容が反映されます。［キャンセル］ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「MAC フィルタリング」のリストのページに戻ります。

8-4 バーチャルサーバ

【バーチャルサーバ機能について】
バーチャルサーバ機能は、インターネット上（リモートホスト）から、LAN 側の接続機器にアクセスを行わせる際に設定する機能です。
通常、LAN に設置されている機器は、ローカル IP アドレスを持っており、グローバル IP アドレスでアクセスを行うことはできません。
バーチャルサーバ機能を利用し、プロトコル・TCP/UDP ポート番号を指定することによって、LAN 内のどの接続機器へ向けての通信であるか特定できるようになるため、グローバル IP アドレスからのアクセスが行えるようになります。
DMZ と同時に使用することはできません。

1. 設定ツールのメニューから、［ネットワーク］－［バーチャルサーバ］をクリックします。
   「バーチャルサーバ」リストのページが表示されます。

ネットワーク
ネットワークの各設定を行います。
バーチャルサーバ
バーチャルサーバの設定を行います。
設定の追加 追加

No.	インターフェイス	プロトコル	開始ポート	終了ポート	サーバのIPアドレス	メモ	操作
1	モバイル通信端末	TCP	80	80	192.168.62.50	http	変更 削除

2. バーチャルサーバ設定の追加を行いたい場合は、［追加］ボタンをクリックします。設定済みの項目を変更する場合は、［変更］をクリックします。［削除］をクリックすると、表示されている設定が削除されます。［追加］ボタン、または［変更］をクリックすると、「バーチャルサーバの詳細設定」ページが表示されます。［追加］ボタンをクリックした場合は空白の状態で、［変更］をクリックした場合は、設定済みの情報が入力された状態で開きます。

バーチャルサーバの設定は最大 32 件まで行えます。

バーチャルサーバの詳細設定

No.	1
インターフェイス	モバイル通信端末
プロトコル	TCP
開始ポート番号	80
終了ポート番号	80
サーバのIPアドレス	192.168.62.50
サーバのポート番号	85
外部からのアクセス	INPUTフィルタリングに従う
メモ	http

設定 キャンセル

3. 以下の設定を行います。

項目	内容
No.	バーチャルサーバ設定の通し番号が表示されます。
インターフェイス	バーチャルサーバの設定を行うインターフェイスを指定します。[モバイル通信端末]、[WAN]、[PPPoE]のいずれかを指定します。
プロトコル	[TCP]、[UDP]、[all]のいずれかを指定します。
開始ポート番号	WAN 側で受け付けるポート番号の範囲を指定します。 ここでは、開始ポート番号を 1～65535 までの番号で指定します。 ▶「＊」などのワイルドカードでの指定は行えません。
終了ポート番号	WAN 側で受け付けるポート番号の範囲を指定します。 ここでは、終了ポート番号を 1～65535 までの番号で指定します。 １つのポート番号しか指定しない場合は、開始ポート番号と同じポート番号を指定します。 ▶「＊」などのワイルドカードでの指定は行えません。
サーバの IP アドレス	バーチャルサーバとして外部に公開する機器の IP アドレスを指定します。
サーバのポート番号	LAN 側のサーバに転送するポート番号を、1～65535 までの番号で指定します。 指定しない場合は「ポート番号」と同じポート番号となります。 ▶「開始ポート番号」「終了ポート番号」で範囲を指定した場合は、サーバの開始ポート番号となります。
外部からのアクセス	WAN 側からのサーバへのアクセスを許可するポリシーを設定します。 [全て許可する]、[INPUT フィルタリングに従う]から選択します。
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶半角 16 文字（全角 8 文字）までの任意の文字列を入力できます。

4. [設定]ボタンをクリックすると、「バーチャルサーバ」リストのページに戻り、設定した内容が反映されます。[キャンセル]ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「バーチャルサーバ」のリストのページに戻ります。

8-5 DMZ

【DMZ 機能について】
DMZ 機能は、バーチャルサーバ機能と同様、インターネット上（リモートホスト）から、LAN 側の接続機器にアクセスを行わせる際に設定する機能ですが、ポート番号が不明な場合でも設定できます。
ポート番号が特定できない通信を行いたい場合などに最適な設定です。ただし、以下の点にご注意願います。

- Rooster RX では、DMZ として設定できる機器は一台のみとなります。
- DMZ として設定された機器には、フィルタリングの設定が全く適用されなくなり、セキュリティが弱くなります。必要な場合のみ設定を行うようにしてください。

➔ フィルタリングの設定については、『8-3　フィルタリング』をご覧ください。

- バーチャルサーバと同時に使用することはできません。

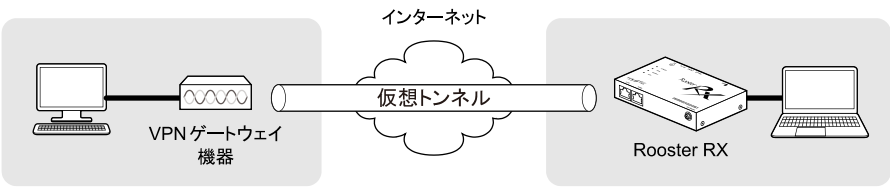
1. 設定ツールのメニューから、［ネットワーク］－［DMZ］をクリックします。

   「DMZ 設定」のページが表示されます。

2. DMZ を使用する場合、［DMZ を使用する］チェックをオンにします。
3. ［DMZ を使用する機器のプライベート IP アドレス］に、DMZ として設定する機器のプライベート IP アドレスを入力します。
4. ［設定］ボタンをクリックして、設定内容を反映させます。

8-6 IPsec

【IPsec について】
IPsec は暗号技術を用いて、IP パケット単位でデータの改ざん防止や秘匿機能を提供するプロトコルです。インターネットなどの公共的なネットワークで、あたかも専用線接続のような、秘匿性の高いネットワークを実現させるためのしくみです。

『8-8　L2TP/IPsec』と同時に使用することはできません。

1. 設定ツールのメニューから、［ネットワーク］－［IPsec］をクリックします。

「IPsec」リストのページが表示されます。

No.	インターフェイス	相手IPアドレス	相手ネットワーク	メモ	操作
1	モバイル通信端末	11.22.33.44	192.168.61.0	IPsec	変更 削除

2. IPsec 設定の追加を行いたい場合は、［追加］ボタンをクリックします。設定済みの項目を変更する場合は、［変更］をクリックします。

「IPsec の詳細設定」ページが表示されます。

memo IPsec の設定は最大 16 件まで行えます。

IPsecの詳細設定

No.	1
インターフェイス	モバイル通信端末
モード設定	メインモード
接続種別	イニシエータ
ハッシュアルゴリズム	SHA-1
暗号化アルゴリズム	3DES
PreSharedKey	test
IKE Life Time	3600 秒
IPsec Life Time	28800 秒
相手IPアドレス	11.22.33.44
相手ネットワーク	192.168.61.0
相手ネットマスク	255.255.255.0
相手側識別子	
Rooster側IPアドレス	
Rooster側ネットワーク	
Rooster側ネットマスク	
Rooster側識別子	
メモ	IPsec

□セッションキープを行う。
□キープアライブを行う。
監視先IPアドレス1
監視先IPアドレス2
□バックアップ設定を使用する。
バックアップ設定

設定 キャンセル

3. 以下の設定を行います。

項目	内容
No.	IPsec 設定の通し番号が表示されます。
インターフェイス	この設定を適用するインターフェイスを選択します。 ［モバイル通信端末］、［WAN］、［PPPoE］から選択します。 バックアップ設定では、動作には無関係です。
モード設定	［メインモード］または［アグレッシブモード］のいずれかを選択します。
接続種別	［イニシエータ］または［レスポンダ］のいずれかを選択します。 ［イニシエータ］は IKE 接続要求を行います。［レスポンダ］は IKE の待ち受けを行います。 バックアップ設定では、動作には無関係です。
ハッシュアルゴリズム	［SHA-1］または［MD5］のいずれかを選択します。 フェーズ 1、フェーズ 2 とも共通の設定になります。
暗号化アルゴリズム	［AES256bit］または［3DES］のいずれかを選択します。
PreSharedKey	IPsec 通信を行うために使用する認証用キーフレーズを設定します。2 点間で同じ値を設定します。
IKE Life Time	IKE の寿命を秒単位で指定します。1081 秒以上で設定してください。
IPsec Life Time	IPsec の寿命を秒単位で指定します。1081 秒以上で設定してください。
相手 IP アドレス	IPsec 通信を行う相手先のグローバル IP アドレスを指定します。ホスト名での指定も可能です。モード設定が［アグレッシブ］で接続種別が［レスポンダ］の場合、相手 IP アドレスには「0.0.0.0」と設定してください。
相手ネットワーク	IPsec 通信を行う相手先のローカルネットワークアドレスを指定します。（相手側 ID）
相手ネットマスク	IPsec 通信を行う相手先のローカル（サブ）ネットマスクアドレスを指定します。（相手側 ID）
相手側識別子	アグレッシブモードで接続する際に、IPsec 通信で互いに相手を識別するために設定します。接続種別で［レスポンダ］を選択された場合に設定し、2 点間で同じ値を設定します。「@」をはさんだ文字列にて指定します。例）test@test
Rooster 側 IP アドレス	メインモードで接続する際に Rooster に割り当てられるグローバル IP アドレスを指定します。ホスト名での指定も可能です。
Rooster 側ネットワーク	Rooster のローカルネットワークアドレスを指定します。 （Rooster 側 ID）
Rooster 側ネットマスク	Rooster のローカル（サブ）ネットマスクアドレスを指定します。 （Rooster 側 ID）
Rooster 側識別子	アグレッシブモードで接続する際に、IPsec 通信で互いに相手を識別するために設定します。接続種別で［イニシエータ］を選択された場合に設定し、2 点間で同じ値を設定します。「@」をはさんだ文字列にて指定します。例）test@test
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶半角 16 文字（全角 8 文字）までの任意の文字列を入力できます。
セッションキープを行う	チェックをオンにした場合、IPsec 接続が切断されると、自動的に再接続を行うようになります。接続種別で［レスポンダ］を選択された場合は、チェックをオンにしても動作いたしません。

項目	内容
キープアライブを行う	IPsec 接続を常時監視し、接続状態を続ける機能です。 チェックをオンにした場合、IPsec 接続時に接続確認のために、設定された監視先 IP アドレスに ping パケットを発信するようになります。 セッションキープ、キープアライブは、従量制課金でご契約の場合は、設定しないようにしてください。意図しない接続で通信料金が掛かってしまう原因となりますので、くれぐれもご注意願います。
バックアップ設定を使用する	上記の設定で接続できなかった場合、代替の設定で接続を行うようにすることができます。代替の設定を使用する場合、チェックをオンにします。接続種別が［レスポンダ］の場合、チェックをオンにしても動作いたしません。

引き続いて［バックアップ設定］も行う場合は、ここで一度、［設定］ボタンをクリックして、設定内容を反映させます。［バックアップ設定］を先にクリックすると、設定した内容が破棄されてしまいます。

4. ［設定］ボタンをクリックすると、「IPsec」リストのページに戻り、設定した内容が反映されます。［キャンセル］ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「IPsec」のリストのページに戻ります。

- 設定が空白の場合、自動的に適切な設定が行われるようになっています。
- IPsec の接続が完了するまでに 1 ～3 分程度かかります。通信を行う前に、ping コマンド等で接続状態を確認することをお勧めします。

他社製 IPsec 機器と接続を行う場合、以下の表を参考に設定を行ってください。

Rooster RX 既定の IPsec 接続設定

項目	既定の設定内容
基本設定	
データ圧縮（IPCOMP プロトコル）	圧縮は使用しない。
鍵交換方式	IKE（Internet Key Exchange）を使って、SA の合意を通信時に自動的に行う。（手動設定は行わない。）
IKE フェーズ 1 （ISAKMP SA の作成） の設定	
接続試行回数	無限回（制限なし）
ハッシュアルゴリズム	SHA-1、MD5
認証方式	Pre-Shared Key（共通鍵）認証方式
Pre-Shared Key （共通鍵）の設定	自分側と相手側両方に、同じキーフレーズを設定。
暗号化アルゴリズム	AES256bit、3DES
Diffie-Hellman-Group	DH Group 2
識別子（ホスト ID）	「@」をはさんだ文字列にて指定
IKE Life Time	経過時間による設定のみ。
IKE フェーズ 2 （IPsec SA の作成） の設定	
セキュリティプロトコル	ESP のみ。
IPsec Life Time	経過時間による設定のみ。
カプセル化モード	トンネリングモード
暗号化アルゴリズム	AES256bit、3DES
ハッシュアルゴリズム	SHA-1、MD5
PFS（Diffie-Hellman の再計算）	行わない。

8-6-1　IPsec通信の接続／切断方法

1. 設定ツールのメニューから、［ステータス］－［IPsec］をクリックします。

   IPsec ステータスのページが表示されます。

ステータス

現在の設定・状態を表示します。

IPsec

IPsec通信の状態を表示します。

No.	相手IPアドレス	相手ネットワーク	メモ	ステータス	操作
1	11.22.33.44	192.168.61.0	IPsec	接続完了	接続 無効

項目		内容
No.		IPsec 設定の通し番号が表示されます。
相手 IP アドレス		IPsec 通信を行う相手先のグローバル IP アドレスが表示されます。
相手ネットワーク		IPsec 通信を行う相手先のローカルネットワークアドレスが表示されます。
メモ		メモに設定された文字列が表示されます。
ステータス		設定した IPsec の現在の状態が表示されます。 ➲ ステータスの詳細については、『ステータス一覧』をご覧ください。
操作	［接続］	接続動作を行います。
	［切断］	切断動作を行います。
	［無効］	設定を無効にします。次回、［有効］をクリックするまで設定内容を使えないようにします。
	［有効］	設定を有効にします。次回、［無効］になっている設定を再度使えるようにします。

ステータス一覧

ステータス表示	状態	VPN ランプの状態
無効	IPsec 設定が無効になっています。	消灯
処理中	IPsec 接続設定を行っています。	消灯
待機中	IPsec 接続設定は行われていますが、IPsec 接続を試みていない状態です。	消灯
接続試行中	IPsec 接続を行おうとしています。この状態が長く続く場合、設定が間違っているか、相手側がオフラインになっている等の問題で接続できない可能性があります。	消灯
接続完了	IPsec 接続が正常に行えた状態です。	点灯

8-6-2　2点間のWAN側IPアドレスが固定の場合

Rooster RXの設定例

8-6-3　WAN側IPアドレスの一方が固定、Rooster RXが動的の場合

Rooster RXの設定例

8-6-4　Rooster RX同士で、ダイナミックDNSを利用した場合

Rooster RX Ⓐの設定例

IPsecの詳細設定

項目	設定値
No.	1
インターフェイス	モバイル通信端末
モード設定	アグレッシブモード
接続種別	レスポンダ
ハッシュアルゴリズム	SHA-1
暗号化アルゴリズム	AES256bit
PreSharedKey	test
IKE Life Time	3600 秒
IPsec Life Time	28800 秒
相手IPアドレス	0.0.0.0
相手ネットワーク	192.168.62.0
相手ネットマスク	255.255.255.0
相手側識別子	test@rooster
Rooster側IPアドレス	
Rooster側ネットワーク	
Rooster側ネットマスク	
Rooster側識別子	
メモ	

☐セッションキープを行う。
☐キープアライブを行う。
監視先IPアドレス1
監視先IPアドレス2
☐バックアップ設定を使用する。
バックアップ設定

設定　キャンセル

Rooster RX Ⓑの設定例

8-7 PPTP

【PPTP について】
PPTP は暗号通信のためのプロトコルです。2 台のコンピュータの間で情報を暗号化して送受信するので、インターネットを通じて安全に情報をやり取りできます。

1. 設定ツールのメニューから、［ネットワーク］－［PPTP］をクリックします。

「PPTP」リストのページが表示されます。

2. 以下の設定を行います。

項目	内容
認証方式	認証方式を選択します。 ▶［MS-CHAPv2］を選択した場合は［PAP］、［CHAP］、［MS-CHAP］は選択できません。
クライアント割り当て IP アドレス	クライアントに割り当てたい IP アドレスを設定します。 • 開始 IP アドレス 割り当てる IP アドレスの開始アドレスを入力します。 • 個数 PPTP で使用する、開始 IP アドレスからのアドレスの個数を指定します。ユーザの個数分指定します。 ▶［開始 IP アドレス］を「192.168.62.100」、［個数］を「10」と設定した場合、「192.168.62.100～192.168.62.109」が、PPTP で使用する IP アドレスの範囲となります。
No.	PPTP 設定の通し番号が表示されます。
ユーザ名	認証させるユーザ名を表示します。
メモ	メモに設定された文字列が表示されます。

3. PPTP 設定の追加を行いたい場合は、［追加］ボタンをクリックします。設定済みの項目を変更する場合は、［変更］をクリックします。［削除］をクリックすると、表示されている設定が削除されます。［追加］ボタン、または［変更］をクリックすると、「PPTP の詳細設定」ページが表示されます。［追加］ボタンをクリックした場合は空白の状態で、［変更］をクリックした場合は、設定済みの情報が入力された状態で開きます。

> memo
> PPTP の設定は最大 16 件まで行えます。

4. 以下の設定を行います。

項目	内容
No.	PPTP 設定の通し番号が表示されます。
ユーザ名	認証させるユーザ名を設定します。
パスワード	認証させるパスワードを設定します。
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶ 半角 16 文字（全角 8 文字）までの任意の文字列を入力できます。

5. ［設定］ボタンをクリックすると、「PPTP」リストのページに戻り、設定した内容が反映されます。［キャンセル］ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「PPTP」のリストのページに戻ります。

8-7-1　PPTP通信のステータス表示

1. 設定ツールのメニューから、［ステータス］－［PPTP］をクリックします。

   PPTP ステータスのページが表示されます。

ステータス

現在の設定・状態を表示します。

PPTP

■ PPTP通信の状態を表示します。

No.	ユーザ名	クライアント割り当て IPアドレス	メモ	ステータス	操作
1	user	192.168.62.100	192.168.62.100	接続完了	切断 無効

項目		内容
No.		PPTP 設定の通し番号が表示されます。
ユーザ名		設定したユーザ名が表示されます。
クライアント割り当て IP アドレス		クライアントに割り当てた IP アドレスが表示されます。
メモ		メモに設定された文字列が表示されます。
ステータス		設定した PPTP の現在の状態が表示されます。 ➲ ステータスの詳細については、『ステータス一覧』をご覧ください。
操作	［接続］	接続動作を行います。
	［切断］	切断動作を行います。
	［無効］	設定を無効にします。次回、［有効］をクリックするまで設定内容を使えないようにします。
	［有効］	設定を有効にします。次回、［無効］になっている設定を再度使えるようにします。

ステータス一覧

ステータス表示	状態	VPN ランプの状態
無効	PPTP 設定が無効になっています。	消灯
処理中	PPTP 接続設定を行っています。	消灯
待機中	PPTP 接続設定は行われていますが、PPTP 接続を試みていない状態です。	消灯
接続完了	PPTP 接続が正常に行えた状態です。	点灯

8-8 L2TP/IPsec

【L2TP/IPsec について】
L2TP/IPsec はパケット全体の暗号化の仕組みを持たない L2TP において IPsec を併用させることで、データの機密性や完全性を確保した VPN を実現します。2 台のコンピュータの間で情報を暗号化して送受信するので、インターネットを通じて安全に情報をやり取りできます。

- 『8-6　IPsec』と同時に使用することはできません。
- WindowsPC より接続する場合、接続できないことがあります。接続できない場合は、弊社ホームページよりレジストリ変更のファイルをダウンロードし、レジストリ変更を行ってください。

1. 設定ツールのメニューから、［ネットワーク］－［L2TP/IPsec］をクリックします。
   「L2TP/IPsec」リストのページが表示されます。

2. L2TP/IPsec を使用する場合、［L2TP/IPsec を使用する］チェックをオンにします。

3. 以下の設定を行います。

項目	内容
IPsec 暗号化方式	［3DES］または［AES256bit］のいずれかを選択します。
IPsec 認証方式	［MD5］または［SHA-1］のいずれかを選択します。

項目	内容
事前認証キー	IPsec 通信を行うために使用する認証用キーフレーズを設定します。2 点間で同じ値を設定します。
PPP 認証方式	PPP 認証方式を選択します。 ［PAP］、［CHAP］、［MS-CHAP］、[MS-CHAPv2]から選択します。（複数選択することもできます。）
クライアント割り当て IP アドレス	クライアントに割り当てたい IP アドレスを設定します。 • 開始 IP アドレス 割り当てる IP アドレスの開始アドレスを入力します。 • 個数 L2TP/IPsec で使用する、開始 IP アドレスからのアドレスの個数を指定します。ユーザの個数分指定します。 ▶［開始 IP アドレス］を「192.168.62.100」、［個数］を「10」と設定した場合、「192.168.62.100～192.168.62.109」が、L2TP/IPsec で使用する IP アドレスの範囲となります。
No.	L2TP/IPsec 設定の通し番号が表示されます。
ユーザ名	認証させるユーザー名を表示します。
メモ	メモに設定された文字列が表示されます。

4. L2TP/IPsec 設定の追加を行いたい場合は、［追加］ボタンをクリックします。設定済みの項目を変更する場合は、［変更］をクリックします。［削除］をクリックすると、表示されている設定が削除されます。［追加］ボタン、または［変更］をクリックすると、「L2TP/IPsec の詳細設定」ページが表示されます。［追加］ボタンをクリックした場合は空白の状態で、［変更］をクリックした場合は、設定済みの情報が入力された状態で開きます。

memo L2TP/IPsec の設定は最大 16 件まで行えます。

5. 以下の設定を行います。

項目	内容
No.	L2TP/IPsec 設定の通し番号が表示されます。
ユーザ名	認証させるユーザ名を設定します。
パスワード	認証させるパスワードを設定します。
メモ	設定内容を分かりやすくするための覚え書きを入力します。 ▶ 半角 16 文字（全角 8 文字）までの任意の文字列を入力できます。

6. ［設定］ボタンをクリックすると、「L2TP/IPsec」リストのページに戻り、設定した内容が反映されます。［キャンセル］ボタンをクリックすると、設定した内容を反映しないで詳細設定ページを閉じ、「L2TP/IPsec」のリストのページに戻ります。

8-8-1 L2TP/IPsec通信のステータス表示

1. 設定ツールのメニューから、［ステータス］－［L2TP/IPsec］をクリックします。

   L2TP/IPsec ステータスのページが表示されます。

ステータス

現在の設定・状態を表示します。

L2TP/IPsec

L2TP/IPsec通信の状態を表示します。

No.	ユーザ名	クライアント割り当てIPアドレス	メモ	ステータス	操作
1	user	192.168.62.100		接続完了	切断 無効

項目		内容
No.		L2TP/IPsec 設定の通し番号が表示されます。
ユーザ名		設定したユーザ名が表示されます。
クライアント割り当て IP アドレス		クライアントに割り当てた IP アドレスが表示されます。
メモ		メモに設定された文字列が表示されます。
ステータス		設定した L2TP/IPsec の現在の状態が表示されます。 ➔ ステータスの詳細については、『ステータス一覧』をご覧ください。
操作	［接続］	接続動作を行います。
	［切断］	切断動作を行います。
	［無効］	設定を無効にします。次回、［有効］をクリックするまで設定内容を使えないようにします。
	［有効］	設定を有効にします。次回、［無効］になっている設定を再度使えるようにします。

ステータス一覧

ステータス表示	状態	VPN ランプの状態
無効	L2TP/IPsec 設定が無効になっています。	消灯
処理中	L2TP/IPsec 接続設定を行っています。	消灯
待機中	L2TP/IPsec 接続設定は行われていますが、L2TP/IPsec 接続を試みていない状態です。	消灯
接続完了	L2TP/IPsec 接続が正常に行えた状態です。	点灯

9章 ログの参照方法

この章では、各動作のログを参照する方法について説明しています。

9-1 パケット通信ログ

工場出荷時状態では、Rooster RX への負荷を軽減させるため、パケット通信ログは記録しない設定になっています。
パケット通信ログを記録させる場合は、［ログ管理］の設定で「ログ管理を行う」のチェックをオンに設定してください。

➔ 設定方法は、『7-8 ログ管理』をご覧ください。

9-1-1 パケット通過ログ

1. 設定ツールのメニューから、［ログ］－［パケット通信ログ］ －［通過ログ］をクリックします。

   パケット通過ログ一覧のページが表示されます。

ログ

ログ表示の各設定を行います。

パケット通信ログ：通過ログ

■ 通過パケットのログ一覧を表示します。

現在の時間は 2013/08/26 10:30:37 ［最新ログ再読込］ ［全てのログ取得］ ［クリア］

No.	記録時間	通信タイプ	発信元IP	発信元ポート	送信先IP	送信先ポート	終了した理由
1	2013/08/26 10:30:15	ICMP	192.168.62.200	0	[illegible]	0	正常終了
2	2013/08/26 10:30:17	ICMP	[illegible]	0	192.168.62.200	0	正常終了
3	2013/08/26 10:30:19	ICMP	192.168.62.200	0	[illegible]	0	正常終了
4	2013/08/26 10:30:19	ICMP	[illegible]	0	192.168.62.200	0	正常終了
5	2013/08/26 10:30:20	ICMP	192.168.62.200	0	[illegible]	0	正常終了
6	2013/08/26 10:30:20	ICMP	[illegible]	0	192.168.62.200	0	正常終了
7	2013/08/26 10:30:21	ICMP	192.168.62.200	0	[illegible]	0	正常終了
8	2013/08/26 10:30:21	ICMP	[illegible]	0	192.168.62.200	0	正常終了
9	2013/08/26 10:30:22	ICMP	192.168.62.200	0	[illegible]	0	正常終了
10	2013/08/26 10:30:22	ICMP	[illegible]	0	192.168.62.200	0	正常終了

項目	内容
No.	ログの通し番号が表示されます。番号が大きくなるほど、より新しいログとなります。 Rooster RX が再起動した場合、1 から開始します。
記録時間	時刻設定がされている場合、ログの発生した時刻が表示されます。
通信タイプ	IP パケットの種別（TCP、UDP、ICMP など）が表示されます。
発信元 IP	通信の起点になる機器の IP アドレスが表示されます。
発信元ポート	通信の起点になる機器の使用ポート番号が表示されます。
送信先 IP	通信の宛先になる機器の IP アドレスが表示されます。
送信先ポート	通信の宛先になる機器の使用ポート番号が表示されます。
終了した理由	通信が終了した理由が表示されます。 • 「正常終了」 正常に通信が行われた時に表示されます。 • 「タイムアウト」 通信セッション確立後、通信が途中で終了、あるいは終了フラグを確認できなかった時に表示されます。

9-1-2　パケット遮断ログ

1. 設定ツールのメニューから、［ログ］－［パケット通信ログ］－［遮断ログ］をクリックします。

   パケット遮断ログ一覧のページが表示されます。

項目	内容
No.	ログの通し番号が表示されます。番号が大きくなるほど、より新しいログとなります。Rooster RX が再起動した場合、1 から開始します。
記録時間	時刻設定がされている場合、ログの発生した時刻が表示されます。
通信タイプ	IP パケットの種別（TCP、UDP、ICMP など）が表示されます。
発信元 IP	通信の起点になる機器の IP アドレスが表示されます。
発信元ポート	通信の起点になる機器の使用ポート番号が表示されます。
送信先 IP	通信の宛先になる機器の IP アドレスが表示されます。
送信先ポート	通信の宛先になる機器の使用ポート番号が表示されます。

9-2 回線ログ

9-2-1 モバイル通信端末ログ

1. 設定ツールのメニューから、［ログ］－［回線ログ］－［モバイル通信端末ログ］をクリックします。

モバイル通信端末ログ一覧のページが表示されます。

ログ

ログ表示の各設定を行います。

回線ログ：モバイル通信端末ログ

■ モバイル通信端末の通信ログ一覧を表示します。

現在の時間は 2013/08/21 16:20:49 最新ログ再読込 全てのログ取得 クリア

No.	記録時間	ログ
1	2013/08/21 16:11:31	モバイル通信端末制御サービスを開始します
2	2013/08/21 16:11:35	モバイル通信端末をu-blox U200として認識しました
3	2013/08/21 16:11:38	--- モバイル通信端末を初期化します ----------
4	2013/08/21 16:11:41	アンテナレベル:強
5	2013/08/21 16:12:13	ダイヤルを行ないます
6	2013/08/21 16:12:13	電話番号:*99***1#
7	2013/08/21 16:12:14	PPP接続開始
8	2013/08/21 16:12:22	PPP接続が確立しました
9	2013/08/21 16:13:26	回線が切断されました
10	2013/08/21 16:13:28	--- モバイル通信端末を初期化します ----------

※上記の図は RX110 の例です。機種によって内容は異なります。

項目	内容
No	ログの通し番号が表示されます。番号が大きくなるほど、より新しいログとなります。 Rooster RX が再起動した場合、1 から開始します。
記録時間	時刻設定がされている場合、ログの発生した時刻が表示されます。
ログ	モバイル通信端末の動作状態が表示されます。ダイヤルアップ接続が正常に行えない場合、以下のログ表示例をご確認いただき、該当する処置を行ってください。 • 「受信：NO CARRIER　回線接続の確立に失敗しました（リザルトエラー）」 以下のいずれかの場合が考えられます。 【ダイヤルアップ接続先の電話番号が間違っている】 正しい電話番号を設定してください。 【電波状態が悪い】 Rooster RX を通信状態のよい場所に移動するか（できるだけ窓側あるいは高い場所）あるいは、しばらく時間を置いてやり直してみてください。 • 「受信：DELAYED　回線接続の確立に失敗しました（リザルトエラー）」 3 分間以内に 3 回以上、同一電話番号に電話を掛けようとすると、モバイル通信端末に発信規制が掛かってしまいます。一旦接続動作を解除して、しばらくお待ちいただいてからお掛け直しください。 • 「PPP 接続でユーザ認証に失敗しました」 ダイヤルアップ接続の ID、パスワードのいずれかに誤りがあります。再度、ダイヤルアップ接続の設定の確認を行ってください。

9-2-2　WANログ

1. 設定ツールのメニューから、［ログ］－［回線ログ］－［WAN ログ］をクリックします。
   WAN ログ一覧のページが表示されます。

ログ

ログ表示の各設定を行います。

回線ログ：WANログ

■ WAN通信のログ一覧を表示します。

現在の時間は 2013/08/30 17:13:49 ［最新ログ再読込］［全てのログ取得］［クリア］

No.	記録時間	ログ
1	2013/08/30 16:25:37	WAN接続を開始します
2	2013/08/30 16:25:37	接続プロセスを開始します
3	2013/08/30 16:25:41	接続に成功しました(IPアドレス：)

項目	内容
No	ログの通し番号が表示されます。番号が大きくなるほど、より新しいログとなります。 Rooster RX が再起動した場合、1 から開始します。
記録時間	時刻設定がされている場合、ログの発生した時刻が表示されます。
ログ	WAN の動作状態が表示されます。

9-2-3　IPsecログ

1. 設定ツールのメニューから、［ログ］－［回線ログ］－［IPsec ログ］をクリックします。

   IPsec ログ一覧のページが表示されます。

ログ

ログ表示の各設定を行います。

回線ログ：IPsecログ

■ IPsec通信のログ一覧を表示します。

現在の時間は　2013/09/17 10:02:44　最新ログ再読込　全てのログ取得　クリア

No.	記録時間	ログ
1	2013/09/17 09:58:10	IPSecプロセスを終了します
2	2013/09/17 09:58:24	KLIPS debug `none'
3	2013/09/17 09:58:25	KLIPS ipsec0 on ppp1 [illegible]/ pointtopoint [illegible]/32 mtu 1500
4	2013/09/17 09:58:25	Starting Pluto subsystem...
5	2013/09/17 09:58:25	...Openswan IPsec started
6	2013/09/17 09:58:26	adjusting ipsec.d to /etc/ipsec.d
7	2013/09/17 09:58:26	Starting Pluto (Openswan Version 2.6.35; Vendor ID OE~HztkoipXB) pid:23268
8	2013/09/17 09:58:26	LEAK_DETECTIVE support [enabled]
9	2013/09/17 09:58:26	OCF support for IKE [disabled]
10	2013/09/17 09:58:26	SAref support [disabled]: Protocol not available
11	2013/09/17 09:58:26	SAbind support [disabled]: Protocol not available
12	2013/09/17 09:58:26	NSS support [disabled]
13	2013/09/17 09:58:26	HAVE_STATSD notification support not compiled in
14	2013/09/17 09:58:26	Setting NAT-Traversal port-4500 floating to off
15	2013/09/17 09:58:26	port floating activation criteria nat_t=0/port_float=1
16	2013/09/17 09:58:26	NAT-Traversal support [disabled]
17	2013/09/17 09:58:26	using /dev/urandom as source of random entropy

項目	内容
No	ログの通し番号が表示されます。番号が大きくなるほど、より新しいログとなります。 Rooster RX が再起動した場合、1 から開始します。
記録時間	時刻設定がされている場合、ログの発生した時刻が表示されます。
ログ	IPsec の動作状態が表示されます。 IPsec 接続が成功すると、「IPsec の No.＊（＊は IPsec 設定リストの No.）が接続完了しました」と表示されます。 接続できない場合、IPsec の設定に誤りがないかどうかご確認ください。 ➲ IPsec の設定につきましては、『8-6　IPsec』をご覧ください。

9-2-4　PPTPログ

1. 設定ツールのメニューから、［ログ］－［回線ログ］－［PPTP ログ］をクリックします。

   PPTP ログ一覧のページが表示されます。

項目	内容
No	ログの通し番号が表示されます。番号が大きくなるほど、より新しいログとなります。Rooster RX が再起動した場合、1 から開始します。
記録時間	時刻設定がされている場合、ログの発生した時刻が表示されます。
ログ	PPTP の動作状態が表示されます。

9-2-5　L2TP/IPsecログ

1. 設定ツールのメニューから、［ログ］－［回線ログ］－［L2TP/IPsec ログ］をクリックします。

   L2TP/IPsec ログ一覧のページが表示されます。

項目	内容
No	ログの通し番号が表示されます。番号が大きくなるほど、より新しいログとなります。Rooster RX が再起動した場合、1 から開始します。
記録時間	時刻設定がされている場合、ログの発生した時刻が表示されます。
ログ	L2TP/IPsec の動作状態が表示されます。

9-3 サービスログ

9-3-1 アドレス解決ログ

1. 設定ツールのメニューから、［ログ］－［サービスログ］－［アドレス解決ログ］をクリックします。

   アドレス解決ログ一覧のページが表示されます。

項目	内容
No	ログの通し番号が表示されます。番号が大きくなるほど、より新しいログとなります。 Rooster RX が再起動した場合、1 から開始します。
記録時間	時刻設定がされている場合、ログの発生した時刻が表示されます。
ログ	アドレス解決機能の動作状態が表示されます。 「アドレス解決プロセスは異常終了しました」となる場合、以下のログ表示例をご確認いただき、該当する処置を行ってください。 【アドレス解決をメール送信で行っている場合】 • 「SMTP サーバエラー: 535 Error: authentication failed」 ユーザ認証 SMTP のメールサーバで、［本体設定］-［メールアカウント設定］の、「アカウント」、「パスワード」のいずれかに誤りがある場合に表示されます。 • 「SMTP サーバエラー: 501 Syntax: MAIL FROM:」 ユーザ認証 SMTP のメールサーバで、［各種サービス］-［アドレス解決］の、「送信元メールアドレス」の設定がされていないか、書式に誤りがある場合に表示されます。 • 「SMTP サーバエラー: 572 Relay not authorized」 POP before SMTP のメールサーバで、［本体設定］-［メールアカウント設定］の「サービスの種類」に「ユーザ認証 SMTP」の設定を行った場合に表示されます。 【アドレス解決を suncomm.DDNS で行っている場合】 • 「suncomm.DDNS サーバエラー」 suncomm.DDNS の設定に誤りがある場合に表示されます。

9-3-2　DHCPログ

1. 設定ツールのメニューから、［ログ］－［サービスログ］－［DHCP ログ］をクリックします。

   DHCP ログ一覧のページが表示されます。

項目	内容
No	ログの通し番号が表示されます。番号が大きくなるほど、より新しいログとなります。Rooster RX が再起動した場合、1 から開始します。
記録時間	時刻設定がされている場合、ログの発生した時刻が表示されます。
ログ	DHCP 機能の動作状態が表示されます。

9-3-3　WANハートビートログ

1. 設定ツールのメニューから、［ログ］－［サービスログ］－［WAN ハートビートログ］をクリックします。

   WAN ハートビートログ一覧のページが表示されます。

項目	内容
No	ログの通し番号が表示されます。番号が大きくなるほど、より新しいログとなります。Rooster RX が再起動した場合、1 から開始します。
記録時間	時刻設定がされている場合、ログの発生した時刻が表示されます。
ログ	WAN ハートビート機能の動作状態が表示されます。

9-3-4　PPPログ

工場出荷時状態では、Rooster RX への負荷を軽減させるため、PPP ログは記録しない設定になっています。
PPP ログを記録させる場合は、［ログ管理］の設定で「PPP ログを有効にする」のチェックをオンに設定してください。

➲ 設定方法は、『7-8　ログ管理』をご覧ください。

1. 設定ツールのメニューから、［ログ］－［サービスログ］－［PPP ログ］をクリックします。

PPP ログ一覧のページが表示されます。

No.	記録時間	ログ
1	2013/08/21 17:20:52	pppd options in effect:
2	2013/08/21 17:20:52	debug # (from /etc/ppp/peers/ppp_client)
3	2013/08/21 17:20:52	kdebug 0 # (from command line)
4	2013/08/21 17:20:52	idle 60 # (from command line)
5	2013/08/21 17:20:52	persist # (from command line)
6	2013/08/21 17:20:52	demand # (from command line)
7	2013/08/21 17:20:52	logfile sclog # (from /etc/ppp/peers/ppp_client)
8	2013/08/21 17:20:52	unit 1 # (from command line)
9	2013/08/21 17:20:52	dump # (from /etc/ppp/peers/ppp_client)
10	2013/08/21 17:20:52	user suncomm # (from command line)
11	2013/08/21 17:20:52	/dev/ttySC0 # (from command line)
12	2013/08/21 17:20:52	115200 # (from command line)
13	2013/08/21 17:20:52	lock # (from command line)
14	2013/08/21 17:20:52	connect /rooster/ondemand.sh # (from command line)

項目	内容
No	ログの通し番号が表示されます。番号が大きくなるほど、より新しいログとなります。Rooster RX が再起動した場合、1 から開始します。
記録時間	時刻設定がされている場合、ログの発生した時刻が表示されます。
ログ	PPP の動作状態が表示されます。

9-4 その他ログ

9-4-1 システムログ

1. 設定ツールのメニューから、［ログ］－［その他ログ］－［システムログ］をクリックします。

   システムログ一覧のページが表示されます。

項目	内容
No	ログの通し番号が表示されます。番号が大きくなるほど、より新しいログとなります。 Rooster RX が再起動した場合、1 から開始します。
記録時間	時刻設定がされている場合、ログの発生した時刻が表示されます。
ログ	Rooster RX のシステムに関するログが表示されます。

本章で紹介したログの参照方法の他に、全てのログを一括でパソコンにアップロードする TELNET コマンドがあります。詳しくは「TELNET 設定機能説明書」をご覧ください。

10章 TELNETコマンドでのみ設定／実行可能な機能

この章では、TELNET コマンドでのみ設定／実行できる機能について説明しています。

10-1 TELNETコマンドでのみ設定／実行可能な機能一覧

TELNET コマンドでのみ設定／実行可能な機能とは、WEB 設定ツールからは設定／実行が行えなく、TELNET コマンドからのみ設定／実行が行える機能です。

- TFTP を利用したファームウェアアップデート（FW Ver1.1.0 以降）
- FTP を利用したファームウェアアップデート
- TFTP を利用した設定ファイルのアップデート（FW Ver1.1.0 以降）
- FTP を利用した設定ファイルのアップデート
- ログファイルのアップロード
- SIM の PIN1 コード設定と PIN1 ロック解除の無効／有効設定
- 通信モジュール自動リセットの無効／有効設定
- 通信モジュール自動リセット時間間隔設定
- 通信モジュールのリセット
- 電話番号の表示
- IMEI（通信モジュール製品番号）の表示
- アンテナレベルの表示、電波品質の表示（ RX110 RX180 のみ、FW Ver1.4.0 以降）
- モバイル通信端末情報一覧の表示
- DHCP リース時間設定
- WAN ハートビートタイムアウト回数の設定
- PING の実行
- 本製品のシリアル番号表示
- ARP キャッシュ表示
- 現在の設定一覧表示
- 温度センサーの温度表示
- 電源電圧の電圧表示
- 位置測位情報の表示（ RX160 のみ、FW Ver1.4.0 以降）
- NTP の状態表示
- ルーティングの状態表示
- 緊急速報の無効／有効設定（ RX130 のみ、FW Ver1.2.0 以降）
- 緊急速報のブロードキャスト設定（ RX130 のみ、FW Ver1.2.0 以降）
- 緊急速報のブロードキャストメッセージの MAGIC WORD 設定（ RX130 のみ、FW Ver1.2.0 以降）
- 緊急速報の表示（ RX130 のみ、FW Ver1.2.0 以降）
- 緊急速報の件数と最終受信時刻表示（ RX130 のみ、FW Ver1.2.0 以降）
- 緊急速報件数のクリア（ RX130 のみ、FW Ver1.2.0 以降）
- 緊急速報の受信テスト（ RX130 のみ、FW Ver1.2.0 以降）

実際の TELNET コマンドの詳細は「TELNET 設定機能説明書」をご覧ください。

付録

製品仕様

項目		仕様	対象
製品名		Rooster RX110（ルースターアールエックス 110） Rooster RX130（ルースターアールエックス 130） Rooster RX160（ルースターアールエックス 160） Rooster RX180（ルースターアールエックス 180）	
型名		SC-RRX110 / SC-RRX130 / SC-RRX160 / SC-RRX180	
JAN コード		4907940130131	RX110
		4907940130186	RX130
		4907940130193	RX160
		4907940130179	RX180
インターフェイス	LAN/WAN ポート	100BASE-TX/10BASE-T×2 ポート（MDI/MDI-X 自動判別）	
	アンテナコネクタ	SMA x1	RX110 RX130 RX180
		SMA x2	RX160
RF インターフェイス	無線周波数	2100/800MHz	RX110 RX130
		800MHz	RX160
		2100/900MHz	RX180
	アクセス方式	WCDMA/HSPA（NTT ドコモ網）	RX110 RX130
		OFDMA/SC-FDMA（KDDI 網）	RX160
		WCDMA/HSDPA（ソフトバンク網）	RX180
	データ通信速度	上り：最大 5.7Mbps 下り：最大 7.2Mbps	RX110 RX130 RX180
		上り：最大 25Mbps 下り：最大 75Mbps	RX160
ハードウェア構成	CPU	メイン：freescale i.MX287（400MHz）	
	メインメモリ	128MB（DDR2）	
	フラッシュメモリ	NOR Flash：3 系統 • 4MB（IPL 用） • 4MB（ログ保存用） • 16MB（ファイルシステム）	
	LED	8 個	
	DIP スイッチ	4 ビット 1 個	
	Push スイッチ	1 個	
	温度センサ	ケース内 2 系統	
	電圧監視	DCIN 電圧 1 系統	
電源	電圧	4.75～29.0V	
	最大消費電力	5W	
	電圧リップル	100mVp-p 以下	
	コネクタ	組込み電源用ハーネスコネクタ（JST PAP-02V-S）	

環境条件	動作温度	-20～60℃
	動作湿度	25～85%（結露なきこと）
	保存温度	-20～70℃
	保存湿度	25～85%（結露なきこと）
	耐ノイズ性（※1） AC ラインノイズ DC ラインノイズ	 ±2000V パルス幅 100ns/1000ns ±2000V パルス幅 100ns/1000ns ノイズシミュレータによる
	耐静電気性（※1） 直接放電 気中放電	 ±10KV LAN/WAN 端子金属部 ±10KV LAN/WAN 端子金属部 （アンテナコネクタを除く）
重量		約 350g（本体のみ）
外形寸法		約 22（H）×81（D）×127（W） 単位 mm （突起部、取付金具除く）
サポートプロトコル	Ethernet	CSMA/CD
	ルーティング	IP のみ
	認証	PAP、CHAP、MS-CHAP、MS-CHAPv2
	WAN プロトコル	PPP
	管理プロトコル	SNMPv1
DHCP	サーバ機能	LAN 側最大 253 クライアント （DNS サーバ IP 指定、リース時間設定可）
	クライアント機能	有線接続
アドレス変換		NAT/IP マスカレード
VPN パススルー		IPsec/PPTP パススルー
サーバ公開		バーチャルサーバ（最大 32 件設定可） DMZ ホスト（1 件設定可）
スタティックルーティングテーブル		最大 128 件登録可能
アップデート		WWW ブラウザによるアップデート telnet によるアップデート（ftp サーバからダウンロード） telnet によるアップデート（tftp サーバからダウンロード）
アドレス解決	アドレス登録	1 件
	メッセージ登録	1 件
	プロトコル	SMTP、POP
	ダイナミック DNS	suncomm.DDNS（※2）
	更新時間設定	可能（5 分～）
WAN ハートビート	相手先	WAN ゲートウェイ、任意のアドレス/ドメイン名設定
	更新時間設定	可能（1 分～）
無通信監視タイマー		設定可能
電源制御		• ハードウェアおよびソフトウェア • モバイル通信端末
ハードウェアウォッチドッグ 信号受信タイミング 発動条件 発動動作		 常時監視（1 秒毎） 信号不受信から 112±16 秒後 本体電源 OFF から 10 秒後に再起動

項目		内容
有線 LAN 接続方式		固定 IP、DHCP、PPPoE（Numbered 接続）
ダイヤルアップ自動発信条件		• LAN 側からのパケット送出 • ダイヤルアップ/セッションキープ • ダイヤルアップ/キープアライブ • IPsec/セッションキープ • IPsec/キープアライブ • WAN ハートビート • NTP
ダイヤルアップ手動発信/切断		可能
ダイヤルアップ先設定		8 件
ダイヤルアップセッションキープ		可能
WAN 側 IP アドレス固定		可能
モバイル通信端末情報		自局電話番号、電界強度、IMEI、ICCID
		電波品質 RX110 RX180
WakeOn		IP 着信、SMS 受信
VPN（IPsec）機能	暗号化	AES256bit、3DES
	アルゴリズム	IKE（メインモード、アグレッシブモード）
	接続要求	イニシエータ、レスポンダ
	接続可能数	最大 16 件
	セッションキープ設定	可能
	キープアライブ設定	可能
	バックアップ設定	別 VPN 装置への接続設定可能 （1 セッションにつき 1 件）
	LifeTime 設定	可能
VPN（PPTP）機能	暗号化	GRE
	接続可能数	最大 16 件
	認証方式	PAP、CHAP、MS-CHAP、MS-CHAPv2
VPN（L2TP/IPsec）機能	IPsec 暗号化	AES256bit、3DES
	IPsec 認証方式	MD5、SHA-1
	接続可能数	最大 16 件
	PPP 認証方式	PAP、CHAP、MS-CHAP、MS-CHAPv2
APN 設定		10 件 RX110 RX130 RX180
		1 件 RX160
ロギング		本体内蔵の不揮発性メモリへ保存 • WWW ブラウザによる各種ログ表示 • telnet による各種ログ表示 • telnet による ftp サーバへの全ログ保存 • Syslog での出力

ログの内容		• パケット通信ログ • パケット遮断ログ • モバイル通信端末ログ • WAN ログ • アドレス解決ログ • WAN ハートビートログ • DHCP ログ • IPsec ログ • PPTP ログ • L2TP/IPsec ログ • PPP ログ • システムログ • 無線 LAN ログ（※4）
設定情報管理		• WWW ブラウザによるファイル保存、読み込み • telnet 上でのコマンドによる読み込み、書き込み • telnet による ftp サーバからの読み込み • telnet による tftp サーバからの読み込み
FORWARD フィルタリング		最大 128 件登録可能 以下の各パラメータによるフィルタリング • インターフェイス • 方向 • 動作（許可または遮断） • プロトコル • 宛先 IP アドレス • 宛先ポート
INPUT フィルタリング		最大 64 件登録可能 以下の各パラメータによるフィルタリング • 動作（許可または遮断） • プロトコル • 相手 IP アドレス • ネットマスク • 相手ポート
MAC フィルタリング		最大 32 件登録可能
インターネット経由のリモートセットアップ		可能
時刻管理	設定方法	NTP サーバ設定/手動設定/通信モジュールより取得
	更新時間設定	可能
おやすみモード	有効条件	待機時
	非活性デバイス	待機時 CPU、LAN/WAN、無線 LAN（※4）、LED（POWER ランプ以外）、温度センサ、電圧センサ、スイッチ類、ログ保存
	動作条件	省電力動作へ • ユーザ指定　曜日、時刻指定 • モバイル通信未接続状態が指定時間続く 通常動作へ • ユーザ指定　曜日、指定時刻 • モバイル通信着信時（IP、SMS）
	消費電力	省電力動作 待機時：0.3W

緊急速報受信	RX130	• 緊急速報のブロードキャスト転送 • 緊急速報の表示 • 緊急速報の件数と最終受信時刻表示 • 緊急速報の受信テスト
位置測位機能	RX160	位置情報の取得
保証		1 年間
付属品		スタートアップマニュアル（保証書付き）（※3）

※1　ノイズを印加し続けた際の動作を保証するものではございません。
※2　suncomm.DDNS は弊社が運用するダイナミック DNS サービスです。
※3　Rooster RX をご利用にあたって電源（AC アダプタ）、外部アンテナ、LAN ケーブルが別途必要となります。
※4　無線 LAN 対応機の場合となります。

最新情報の入手

Rooster RX に関する最新情報は、弊社ホームページから入手することができます。また、バージョンアップ情報につきましても公開しております。

- 製品紹介ページ
  http://www.sun-denshi.co.jp/sc/rx/

ご質問･お問い合わせ

Rooster RX に関するご質問やお問い合わせは、下記へご連絡願います。

ユーザーサポートセンター

- 電話　0587-55-0161
- FAX　0587-55-0815
- メール　support-suncomm@sun-denshi.co.jp
- 受付時間　月曜～金曜　10:00～16:00（12:00～13:00 を除く）
  祝日、弊社休日を除く

Rooster RX 取扱説明書　Ver.1.4.0

サン電子株式会社
2014 年 10 月発行　(141007)